Часть I

Конечные поля (поля Галуа) I

Разделы

Поле $GF(p)$

- $\mathbb{Z}$ — кольцо целых чисел евклидово (целостное унитальное + возможно деление с остатком $\Rightarrow$ существование НОД!),
- p — простое число.
- $(p) = \{ np \mid n \in \mathbb{Z} \} = p\mathbb{Z} = \{ 0, \pm p, \pm 2p, \dots \}$ — *идеал*
- $\mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z} = \{ \overline{0}, \overline{1}, \dots, \overline{p-1} \}$ — кольцо вычетов по модулю этого идеала = классы остатков от деления на p:

$$\left.\begin{array}{ll} \overline{0} & = 0 + p\mathbb{Z}\,, \\ \overline{1} & = 1 + p\mathbb{Z}\,, \\ \dots & \dots\dots \\ \overline{p-1} & = (p-1) + p\mathbb{Z}\,. \end{array}\right\} \Rightarrow \mathbb{Z} = \overline{0} \cup \overline{1} \cup \dots \cup \overline{p-1}.$$

Черту над символами классов вычетов часто не ставят.

Поле $GF(p)$

- $\mathbb{Z}$ — кольцо целых чисел евклидово (целостное унитальное + возможно деление с остатком $\Rightarrow$ существование НОД!),
- p — простое число.
- $(p) = \{ np \mid n \in \mathbb{Z} \} = p\mathbb{Z} = \{ 0, \pm p, \pm 2p, \dots \}$ — *идеал*
- $\mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z} = \{ \overline{0}, \overline{1}, \dots, \overline{p-1} \}$ — кольцо вычетов по модулю этого идеала = классы остатков от деления на p:

$$\left.\begin{array}{ll} \overline{0} & = 0 + p\mathbb{Z}\,, \\ \overline{1} & = 1 + p\mathbb{Z}\,, \\ \dots & \dots\dots \\ \overline{p-1} & = (p-1) + p\mathbb{Z}\,. \end{array}\right\} \Rightarrow \mathbb{Z} = \overline{0} \cup \overline{1} \cup \dots \cup \overline{p-1}.$$

Черту над символами классов вычетов часто не ставят.

Поскольку p — простое, то $\mathbb{Z}/(p)$ — не просто кольцо, а поле (возможно деление без остатка на любой ненулевой элемент). Это простейшее *поле Галуа* (простое поле), обозначение — $\mathbb{F}_p$ или $GF(p)$; все операции в нём — по $\mod p$.

Поле $\mathbb{F}_3 = \mathbb{Z}/(3)$ и фактор-кольцо $\mathbb{Z}/(4)$

$\mathbb{F}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Поле $\mathbb{F}_3 = \mathbb{Z}/(3)$ и фактор-кольцо $\mathbb{Z}/(4)$

$\mathbb{F}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}/(4)$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	$\mathbf{0}$	2
3	0	3	2	1

Дважды два равно нулю!

Поле $\mathbb{F}_3 = \mathbb{Z}/(3)$ и фактор-кольцо $\mathbb{Z}/(4)$

$\mathbb{F}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}/(4)$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	$\mathbf{0}$	2
3	0	3	2	1

Дважды два равно нулю!

Однако, поле из 4 элементов существует...

Характеристика поля

Пусть $\Bbbk$ — произвольное поле, 1 — единица $\Bbbk$. Складываем единицы: $1 = 1\,, \quad 2 = 1 + 1\,, \quad \ldots$.

Характеристика поля

Пусть $\Bbbk$ — произвольное поле, 1 — единица $\Bbbk$. Складываем единицы: $1 = 1\,, \quad 2 = 1 + 1\,, \quad \ldots$.

В конечном поле всегда найдётся первое k такое, что

$$\underbrace{1 + \ldots + 1}_{k \text{ раз}} = 0.$$

Тогда k — *порядок аддитивной группы поля* $\Bbbk$ $=$

$$= \textit{характеристика поля } \Bbbk \stackrel{\text{def}}{=} \operatorname{char} \Bbbk$$

$\{\, 0,\, 1,\, 2,\, \ldots,\, (\operatorname{char} \Bbbk - 1) \,\}$ — минимальное подполе поля $\Bbbk$.

Характеристика поля

Пусть $\Bbbk$ — произвольное поле, 1 — единица $\Bbbk$. Складываем единицы: $1 = 1\,, \quad 2 = 1 + 1\,, \quad \ldots$.

В конечном поле всегда найдётся первое k такое, что

$$\underbrace{1 + \ldots + 1}_{k \text{ раз}} = 0.$$

Тогда k — *порядок аддитивной группы поля* $\Bbbk$ $=$

$$= \textit{характеристика поля } \Bbbk \stackrel{\text{def}}{=} \operatorname{char} \Bbbk$$

$\{\, 0,\, 1,\, 2,\, \ldots,\, (\operatorname{char} \Bbbk - 1) \,\}$ — минимальное подполе поля $\Bbbk$.

Если все суммы вида $1 + \ldots + 1$ различны, то $\operatorname{char} \Bbbk = 0$.

Примеры: $\mathbb{Q}$, $\mathbb{R}$ — поля нулевой (или бесконечной :)) характеристики.

Бесконечное поле с положительной характеристикой

Бесконечное поле с положительной характеристикой

$\Bbbk$ — произвольное (конечное или бесконечное) поле. Построим:

1. $\Bbbk[x]$ — кольцо многочленов от формальной переменной x:
$\{ P(x) = a_0 + a_1 x + \ldots + a_n x^n \mid a_0, \ldots, a_n \in \Bbbk,\ a_n \neq 0 \}$;
$\Bbbk[x] \leftrightarrow \{(a_0, \ldots, a_n) \in \Bbbk^n \mid n \in \mathbb{N}\}$.

Бесконечное поле с положительной характеристикой

$\Bbbk$ — произвольное (конечное или бесконечное) поле. Построим:

1. $\Bbbk[x]$ — кольцо многочленов от формальной переменной x:
   $\{ P(x) = a_0 + a_1 x + \ldots + a_n x^n \mid a_0, \ldots, a_n \in \Bbbk,\ a_n \neq 0 \}$;
   $\Bbbk[x] \leftrightarrow \{(a_0, \ldots, a_n) \in \Bbbk^n \mid n \in \mathbb{N}\}$.

2. $\Bbbk(x)$ — поле рациональных функций над $\Bbbk$

Бесконечное поле с положительной характеристикой

$\Bbbk$ — произвольное (конечное или бесконечное) поле. Построим:

1. $\Bbbk[x]$ — кольцо многочленов от формальной переменной x:
   $\{ P(x) = a_0 + a_1 x + \ldots + a_n x^n \mid a_0, \ldots, a_n \in \Bbbk,\ a_n \neq 0 \}$;
   $\Bbbk[x] \leftrightarrow \{(a_0, \ldots, a_n) \in \Bbbk^n \mid n \in \mathbb{N}\}$.

2. $\Bbbk(x)$ — поле рациональных функций над $\Bbbk$; в нём:
   элементы — "дроби" P/Q (если $Q \neq 0$), где $P, Q \in \Bbbk[x]$;
   умножение — $(P/Q) \cdot (U/V) = (PU)/(QV)$;
   эквивалентность — $P_1/Q_1 = P_2/Q_2$, если $P_1 Q_2 = P_2 Q_1$;
   сложение — дроби можно приводить к общему знаменателю и складывать:
   $$P/Q + U/V = (PV)/(QV) + (QU)/(QV) = (PV + QU)/(QV);$$
   включение — Поскольку $\Bbbk[x] \subset \Bbbk(x)$, то каждый многочлен P отождествляется с $P/1$.

Бесконечное поле с положительной характеристикой

$\Bbbk$ — произвольное (конечное или бесконечное) поле. Построим:

1. $\Bbbk[x]$ — кольцо многочленов от формальной переменной x:
   $\{ P(x) = a_0 + a_1 x + \ldots + a_n x^n \mid a_0, \ldots, a_n \in \Bbbk,\ a_n \neq 0 \}$;
   $\Bbbk[x] \leftrightarrow \{(a_0, \ldots, a_n) \in \Bbbk^n \mid n \in \mathbb{N}\}$.

2. $\Bbbk(x)$ — поле рациональных функций над $\Bbbk$; в нём:
   элементы — "дроби" P/Q (если $Q \neq 0$), где $P, Q \in \Bbbk[x]$;
   умножение — $(P/Q) \cdot (U/V) = (PU)/(QV)$;
   эквивалентность — $P_1/Q_1 = P_2/Q_2$, если $P_1 Q_2 = P_2 Q_1$;
   сложение — дроби можно приводить к общему знаменателю и складывать:
   $$P/Q + U/V = (PV)/(QV) + (QU)/(QV) = (PV + QU)/(QV);$$
   включение — Поскольку $\Bbbk[x] \subset \Bbbk(x)$, то каждый многочлен P отождествляется с $P/1$.

Если в качестве $\Bbbk$ взять конечное поле $\mathbb{F}_p$, то
$\mathbb{F}_p(x)$ — бесконечное поле положительной характеристики p.

Вычисления в поле положительной характеристики

Лемма (об упрощение вычислений)

В поле характеристики $p > 0$ выполнено тождество

$$(a + b)^p = a^p + b^p.$$

Вычисления в поле положительной характеристики

Лемма (об упрощение вычислений)

В поле характеристики $p > 0$ выполнено тождество

$$(a+b)^p = a^p + b^p.$$

Доказательство

В любом коммутативном кольце верна формула для бинома

$$(a+b)^p = \underbrace{a^p + C_p^1 a^{p-1}b + \ldots + C_p^{p-1} ab^{p-1}}_{=0} + b^p,$$

а при $i = 1, \ldots, p-1$ числитель коэффициента $C_p^i = \frac{p!}{i!(p-i)!}$ делится на p, а знаменатель — нет, откуда $C_p^i \equiv_p 0$.

Вычисления в поле положительной характеристики

Лемма (об упрощение вычислений)

В поле характеристики $p > 0$ выполнено тождество

$$(a+b)^p = a^p + b^p.$$

Доказательство

В любом коммутативном кольце верна формула для бинома

$$(a+b)^p = \underbrace{a^p + C_p^1 a^{p-1}b + \ldots + C_p^{p-1} ab^{p-1}}_{=0} + b^p,$$

а при $i = 1, \ldots, p-1$ числитель коэффициента $C_p^i = \frac{p!}{i!(p-i)!}$ делится на p, а знаменатель — нет, откуда $C_p^i \equiv_p 0$.

Следствие

В поле характеристики $p > 0$ справедливо $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

Мультипликативная группа и примитивный элемент поля $\mathbb{F}_p$

$\mathbb{F}_p^* \stackrel{\text{def}}{=} \mathbb{F}_p \setminus \{0\}$ — *мультипликативная группа поля* $\mathbb{F}_p$.

Мультипликативная группа и примитивный элемент поля $\mathbb{F}_p$

$\mathbb{F}_p^* \stackrel{\text{def}}{=} \mathbb{F}_p \setminus \{0\}$ — *мультипликативная группа поля* $\mathbb{F}_p$.

Утверждение

$\mathbb{F}_p^*$ — *циклическая группа порядка* $p-1$

Мультипликативная группа и примитивный элемент поля $\mathbb{F}_p$

$\mathbb{F}_p^* \stackrel{\text{def}}{=} \mathbb{F}_p \setminus \{0\}$ — *мультипликативная группа поля* $\mathbb{F}_p$.

Утверждение

$\mathbb{F}_p^*$ — *циклическая группа порядка* $p-1$ *(по умножению).*

Мультипликативная группа и примитивный элемент поля $\mathbb{F}_p$

$\mathbb{F}_p^* \stackrel{\text{def}}{=} \mathbb{F}_p \setminus \{0\}$ — *мультипликативная группа поля* $\mathbb{F}_p$.

Утверждение

$\mathbb{F}_p^*$ — *циклическая группа порядка* $p-1$ *(по умножению).*

Как любая конечная циклическая группа, $\mathbb{F}_p^*$ содержит генератор = примитивный элемент α:

- любой элемент $\beta \in \mathbb{F}_p^*$ является некоторой его натуральной степенью: $\beta = \alpha^i,\ i \in \{1, \ldots, p-1\}$;
- причём $1 = \alpha^{p-1}$ — т.е. $\alpha^i \neq 1$ для $1 \leqslant i \leqslant p-2$.

Мультипликативная группа и примитивный элемент поля $\mathbb{F}_p$

$\mathbb{F}_p^* \stackrel{\text{def}}{=} \mathbb{F}_p \setminus \{0\}$ — *мультипликативная группа поля* $\mathbb{F}_p$.

Утверждение

$\mathbb{F}_p^*$ — *циклическая группа порядка* $p-1$ *(по умножению).*

Как любая конечная циклическая группа, $\mathbb{F}_p^*$ содержит генератор = примитивный элемент α:

- любой элемент $\beta \in \mathbb{F}_p^*$ является некоторой его натуральной степенью: $\beta = \alpha^i,\ i \in \{1, \ldots, p-1\}$;
- причём $1 = \alpha^{p-1}$ — т.е. $\alpha^i \neq 1$ для $1 \leqslant i \leqslant p-2$.

Утверждение

Группа $\mathbb{F}_p^*$ *имеет* $\varphi(p-1)$ *примитивных элементов.*

Пример: мультипликативная группа поля $\mathbb{F}_{11}$

$\mathbb{F}_{11}^* = \{1, 2, \ldots, 10\}$, число генераторов — $\varphi(10) = 4$.

❶ $\mathbb{F}_{11}^* \cong \langle \{1, 2 \ldots, 10\}, \times_{11} \rangle$

$\langle 1 \rangle = \{1\}$, $\langle 2 \rangle = \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$,

$\langle 3 \rangle = \{3, 9, 5, 4, 1\}$ $(2^{10} = 1024 \equiv_{11} = 1)$ $\ldots$

ещё генераторы: 6, 7, 8

❷ $\mathbb{F}_{11}^* \cong \langle \{0, 1, \ldots, 9\}, +_{10} \rangle$:

$\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\}$,

$\langle 2 \rangle = \{2, 4, 6, 8, 0\}$ $\ldots$

ещё генераторы: 3, 7, 9

Как найти примитивные элементы поля $\mathbb{F}_p$?

Если примарное разложение $p-1$

Как найти примитивные элементы поля $\mathbb{F}_p$?

Если примарное разложение $p-1$

1) известно — элемент $\alpha \in \mathbb{F}_p$ примитивен iff

$$\alpha^{\frac{p-1}{q}} \not\equiv_p 1 \text{ для каждого простого } q \mid (p-1)$$

(т.к. $\alpha^{k \deg \alpha} = 1, k \in \mathbb{N}$).

Как найти примитивные элементы поля $\mathbb{F}_p$?

Если примарное разложение $p-1$

1) известно — элемент $\alpha \in \mathbb{F}_p$ примитивен iff

$$\alpha^{\frac{p-1}{q}} \not\equiv_p 1 \text{ для каждого простого } q \mid (p-1)$$

(т.к. $\alpha^{k \deg \alpha} = 1, k \in \mathbb{N}$).

Пример: $p = 11,\ p-1 = 10 = 2 \cdot 5,\ q \in \{2, 5\}$

$$2^2 = 4,\ 2^5 = 32 \equiv_{11} 10 \Rightarrow 2 \text{ — примитивный}$$

$$3^2 = 9,\ 3^5 = 243 \equiv_{11} 1 \Rightarrow 3 \text{ — не примитивный}$$

Как найти примитивные элементы поля $\mathbb{F}_p$?

Если примарное разложение $p-1$

1) известно — элемент $\alpha \in \mathbb{F}_p$ примитивен iff

$$\alpha^{\frac{p-1}{q}} \not\equiv_p 1 \text{ для каждого простого } q \mid (p-1)$$

(т.к. $\alpha^{k \deg \alpha} = 1, k \in \mathbb{N}$).

Пример: $p = 11,\ p-1 = 10 = 2 \cdot 5,\ q \in \{2, 5\}$

$$2^2 = 4,\ 2^5 = 32 \equiv_{11} 10 \Rightarrow 2 \text{ — примитивный}$$

$$3^2 = 9,\ 3^5 = 243 \equiv_{11} 1 \Rightarrow 3 \text{ — не примитивный}$$

2) неизвестно — эффективного алгоритма не найдено

(используют таблицы, вероятностные алгоритмы...).

Как найти примитивные элементы поля $\mathbb{F}_p$...

Если найден один примитивный элемент α поля $\mathbb{F}_p$, то любой другой его примитивный элемент может быть получен как степень α^k, где k — взаимно просто с $p-1$.

Пример: $p = 11$, 2 — примитивный элемент $\mathbb{F}_{11}$
$k \in \{1, 3, 7, 9\}$ — взаимно простые с $p - 1 = 10$

$$
\begin{aligned}
2^1 &= 2, \\
2^3 &= 8, \\
2^7 &= 128 \equiv_{11} 7, \\
2^9 &= 512 \equiv_{11} 6.
\end{aligned}
$$

Деление с остатком в кольце многочленов над полем

Утверждение

Кольцо многочленов $\Bbbk[x]$ над полем $\Bbbk$ — евклидово.

— значит, многочлены можно делить друг на друга с остатком.
Например, в кольце $\mathbb{F}_2[x]$ —

$$\begin{array}{r|l} x^4 & x^2+1 \\ \underline{x^4+x^2} & \hline x^2+1 \\ x^2 & \\ \underline{x^2+1} & \\ 1 & \end{array}$$

т.е. $x^4 = (x^2+1)^2 + 1$.

Упражнение: делением многочленов «уголком» покажите, что частное от деления многочлена $2x^5 + x^4 + 4x + 3$ на многочлен $3x^2 + 1$ в поле $\mathbb{F}_5[x]$ есть $4x^3 + 2x^2 + 2x + 1$, а остаток — $2x + 2$.

Неприводимые многочлены

Теорема

Каждый элемент евклидова кольца однозначно с точностью до перестановок разлагается в произведение простых элементов.

Простые (неразложимые) элементы колец $\mathbb{k}[x]$ имеют специальное название — *неприводимые многочлены*.

Неприводимые многочлены

Теорема

Каждый элемент евклидова кольца однозначно с точностью до перестановок разлагается в произведение простых элементов.

Простые (неразложимые) элементы колец $\Bbbk[x]$ имеют специальное название — *неприводимые многочлены*.

Свойство «неприводимости» зависит от поля:

многочлен x^4+1 неприводим над $\mathbb{Q}$, но приводим над $\mathbb{F}_2$:

$$x^4+1 = (x^3+x^2+x+1)(x+1).$$

Вопросы для полей:

1. какие многочлены над ними неприводимы?
2. как находить неприводимые многочлены?

Неприводимые многочлены над $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$:

Неприводимые многочлены над $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$:

в поле $\mathbb{C}$ — только многочлены 1-й степени;

Неприводимые многочлены над $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$:

в поле $\mathbb{C}$ — только многочлены 1-й степени;

в поле $\mathbb{R}$ —

1. многочлены 1-й степени,
2. многочлены 2-й степени с отрицательным дискриминантом;

Неприводимые многочлены над $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$:

в поле $\mathbb{C}$ — только многочлены 1-й степени;

в поле $\mathbb{R}$ —

1. многочлены 1-й степени,
2. многочлены 2-й степени с отрицательным дискриминантом;

в поле $\mathbb{Q}$ — существуют неприводимые многочлены произвольной степени.

Далее нас будут интересовать неприводимые многочлены в конечных полях.

Неприводимые многочлены над $\mathbb{F}_2$

Пример

Дано: поле $\mathbb{F}_2 = \langle \{0, 1\}, +_2, \cdot_2 \rangle$.

Требуется: найти все неприводимые многочлены степеней $2, 3, 4$ над ним.

Неприводимые многочлены над $\mathbb{F}_2$

Пример

Дано: поле $\mathbb{F}_2 = \langle \{0,1\}, +_2, \cdot_2 \rangle$.
Требуется: найти все неприводимые многочлены степеней $2, 3, 4$ над ним.

Вторая степень: $x^2 + ax + b$

Ясно, что $b = 1$, иначе $x^2 + ax = x(x + a) \Rightarrow$ ищем неприводимый многочлен в виде $x^2 + ax + 1$.
Если

$a = 0$, то $x^2 + 1 = (x + 1)^2$;

$a = 1$, то получаем

единственный неприводимый многочлен степени 2 над $\mathbb{F}_2$:

$$x^2 + x + 1$$

Неприводимые многочлены над $\mathbb{F}_2$

Третья степень: $x^3 + ax^2 + bx + 1$

(почему свободный член не равен нулю?)

Исключая, как сделано ранее, делимость на $x + 1$, получаем условие $a + b \neq 0$, т.е.

$$\left[\begin{array}{l} a = 0,\ b = 1\,, \\ a = 1,\ b = 0\,. \end{array}\right.$$

Неприводимые многочлены над $\mathbb{F}_2$

Третья степень: $x^3 + ax^2 + bx + 1$

(почему свободный член не равен нулю?)

Исключая, как сделано ранее, делимость на $x + 1$, получаем условие $a + b \neq 0$, т.е.

$$\left[\begin{array}{l} a = 0,\ b = 1\,, \\ a = 1,\ b = 0\,. \end{array}\right.$$

$\therefore$ над $\mathbb{F}_2$ существует два неприводимых многочлена степени 3:

$$x^3 + x^2 + 1 \quad \text{и} \quad x^3 + x + 1\,.$$

Неприводимые многочлены над $\mathbb{F}_2$

Четвёртая степень: $x^4 + ax^3 + bx^2 + cx + 1$

Исключение делимости на $x + 1$ приводит к условию $a + b + c = 1$, т.е. имеется 4 варианта, которые дают 3 решения:

a	b	c	многочлен	
0	0	1	$x^4 + x + 1$	
0	1	0	$x^4 + x^2 + 1$	— приводимый
1	0	0	$x^4 + x^3 + 1$	
1	1	1	$x^4 + x^3 + x^2 + x + 1$	

Откуда взялся ещё один приводимый многочлен?

Неприводимые многочлены над $\mathbb{F}_2$

Четвёртая степень: $x^4 + ax^3 + bx^2 + cx + 1$

Исключение делимости на $x + 1$ приводит к условию $a + b + c = 1$, т.е. имеется 4 варианта, которые дают 3 решения:

a	b	c	многочлен	
0	0	1	$x^4 + x + 1$	
0	1	0	$x^4 + x^2 + 1$	— приводимый
1	0	0	$x^4 + x^3 + 1$	
1	1	1	$x^4 + x^3 + x^2 + x + 1$	

Откуда взялся ещё один приводимый многочлен?
Найдены многочлены, у которых нет линейных делителей (степени 1). Но многочлен 4-й степени может разлагаться в произведение двух неприводимых многочленов 2-й степени:

$$x^4 + x^2 + 1 = (x^2 + x + 1)^2.$$

Неприводимые многочлены над $\mathbb{F}_3$

Поле $\mathbb{F}_3 = \left\langle \{0,1,2\}, +_3, \cdot_3 \right\rangle \Rightarrow$ кольцо многочленов $\mathbb{F}_3[x]$.

Неприводимые многочлены над $\mathbb{F}_3$

Поле $\mathbb{F}_3 = \left\langle \{0,1,2\}, +_3, \cdot_3 \right\rangle \Rightarrow$ кольцо многочленов $\mathbb{F}_3[x]$.
Многочлены порядка 1:

$$x \qquad 2x$$
$$x+1 \qquad 2x+1$$
$$x+2 \qquad 2x+2$$

Какие из них неприводимы?

Неприводимые многочлены над $\mathbb{F}_3$

Поле $\mathbb{F}_3 = \left\langle \{0,1,2\}, +_3, \cdot_3 \right\rangle \Rightarrow$ кольцо многочленов $\mathbb{F}_3[x]$.
Многочлены порядка 1:

$$x \qquad 2x$$
$$x+1 \qquad 2x+1$$
$$x+2 \qquad 2x+2$$

Какие из них неприводимы? Все!

Неприводимые многочлены над $\mathbb{F}_3$

Поле $\mathbb{F}_3 = \left\langle \{0,1,2\}, +_3, \cdot_3 \right\rangle \Rightarrow$ кольцо многочленов $\mathbb{F}_3[x]$.
Многочлены порядка 1:

$$x \qquad 2x$$
$$x+1 \qquad 2x+1$$
$$x+2 \qquad 2x+2$$

Какие из них неприводимы? Все!

Неприводимые многочлены порядка 2 в $\mathbb{F}_3[x]$ (они не имеют корней 0, 1, 2):

$$x^2+1 \qquad 2x^2+2$$
$$x^2+x+2 \qquad 2x^2+x+1$$
$$x^2+2x+2 \qquad 2x^2+2x+1$$

Существование и нахождение неприводимых многочленов

Теорема (о существовании неприводимых многочленов)

Для любых натурального n и простого p над $\mathbb{F}_p$ существует неприводимый многочлен степени n.

Существование и нахождение неприводимых многочленов

Теорема (о существовании неприводимых многочленов)

Для любых натурального n и простого p над $\mathbb{F}_p$ существует неприводимый многочлен степени n.

— докажем позже.

Существование и нахождение неприводимых многочленов

Теорема (о существовании неприводимых многочленов)

Для любых натурального n и простого p над $\mathbb{F}_p$ существует неприводимый многочлен степени n.

— докажем позже.

Вопрос

Как в кольце $\mathbb{F}_p[x]$ найти неприводимый многочлен?

Существование и нахождение неприводимых многочленов

Теорема (о существовании неприводимых многочленов)

Для любых натурального n и простого p над $\mathbb{F}_p$ существует неприводимый многочлен степени n.

— докажем позже.

Вопрос

Как в кольце $\mathbb{F}_p[x]$ найти неприводимый многочлен?

Ответ: нет эффективных алгоритмов 

Существование и нахождение неприводимых многочленов

Теорема (о существовании неприводимых многочленов)

Для любых натурального n и простого p над $\mathbb{F}_p$ существует неприводимый многочлен степени n.

— докажем позже.

Вопрос

Как в кольце $\mathbb{F}_p[x]$ найти неприводимый многочлен?

Ответ: нет эффективных алгоритмов 

(из таблиц, алгоритм из 5-й главы «Алгебры» Ван дер Вардена, алгоритм Берлекэмпа...)

Существование и нахождение неприводимых многочленов

Теорема (о существовании неприводимых многочленов)

Для любых натурального n и простого p над $\mathbb{F}_p$ существует неприводимый многочлен степени n.

— докажем позже.

Вопрос

Как в кольце $\mathbb{F}_p[x]$ найти неприводимый многочлен?

Ответ: нет эффективных алгоритмов 
(из таблиц, алгоритм из 5-й главы «Алгебры» Ван дер Вардена, алгоритм Берлекэмпа...)

Если многочлен не имеет корней, это ещё не значит, что он неприводим. Почему?

Зачем нужны неприводимые многочлены?

Зачем нужны неприводимые многочлены?

Используя неприводимые многочлены, можно строить новые конечные поля — *расширения* простых полей $\mathbb{F}_p$

Зачем нужны неприводимые многочлены?

Используя неприводимые многочлены, можно строить новые конечные поля — *расширения* простых полей $\mathbb{F}_p$:

1. Выбираем простое p и фиксируем поле
$$\mathbb{F}_p = \langle \{0, 1, \ldots, p-1\}, +_p, \cdot_p \rangle.$$
2. Рассматриваем кольцо $\mathbb{F}_p[x]$ многочленов над $\mathbb{F}_p$.
3. Выбираем натуральное n и неприводимый многочлен
$$a(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{F}_p[x].$$
4. Идеал $(a(x))$ порождает фактормножество $\mathbb{F}_p[x]/(a(x))$, элементы которого суть совокупность $\{r(x)\}$ остатков от деления многочленов $f \in \mathbb{F}_p[x]$ на $a(x)$:
$$f(x) = a(x) \cdot q(x) + r(x).$$

Утверждение: множество $\{r(x)\}$ является полем Галуа $GF(p^n)$.

Построение конечных полей...

Доказательство

1. *Кольцо многочленов* $\mathbb{F}_p[x]$ *евклидово, идеал* $(a(x))$ — *максимальный* $\Rightarrow$ $\{r(x)\}$ — *поле.*
2. *Его мощность* $\left|\{r(x)\}\right| =$ *число многочленов над* $\mathbb{F}_p$ *степени не выше* $n-1$, *т.е.* $\left|\{r(x)\}\right| = p^n$.

Построение конечных полей...

Доказательство

1. *Кольцо многочленов* $\mathbb{F}_p[x]$ *евклидово, идеал* $(a(x))$ — *максимальный* $\Rightarrow$ $\{r(x)\}$ — *поле.*
2. *Его мощность* $\left|\{r(x)\}\right| =$ *число многочленов над* $\mathbb{F}_p$ *степени не выше* $n-1$, *т.е.* $\left|\{r(x)\}\right| = p^n$.

Поле $\{r(x)\} = GF(p^n)$ называется *расширением* n*-й степени поля* $\mathbb{F}_p$; альтернативное обозначение — $\mathbb{F}_p^n$.

Вопрос

Почему в обозначении $\mathbb{F}_p^n$ *не используется многочлен* $a(x)$, *с помощью которого построено поле?*

Построение конечных полей...

Доказательство

1. *Кольцо многочленов* $\mathbb{F}_p[x]$ *евклидово, идеал* $(a(x))$ — *максимальный* $\Rightarrow$ $\{r(x)\}$ — *поле.*
2. *Его мощность* $\left|\{r(x)\}\right| =$ *число многочленов над* $\mathbb{F}_p$ *степени не выше* $n-1$, *т.е.* $\left|\{r(x)\}\right| = p^n$.

Поле $\{r(x)\} = GF(p^n)$ называется *расширением* n*-й степени поля* $\mathbb{F}_p$; альтернативное обозначение — $\mathbb{F}_p^n$.

Вопрос

Почему в обозначении $\mathbb{F}_p^n$ *не используется многочлен* $a(x)$, *с помощью которого построено поле?*

Теорема

Любое конечное поле изоморфно какому-нибудь полю Галуа $\mathbb{F}_p^n$.

Пример: построение поля $\mathbb{F}_3^2$

Выберем неприводимый многочлен в $\mathbb{F}_3[x]$: x^2+1.
Искомое поле есть

$$\mathbb{F}_3^2 \cong \mathbb{F}_3[x]/\left(x^2+1\right) = \\ = \{\,0,\,1,\,2,\,x,\,x+1,\,x+2,\,2x,\,2x+1,\,2x+2\,\}.$$

Можно составить таблицы сложения и умножения в этом поле с учётом $x^2 = -1 \equiv_3 2$.
Например:

$$(x+1)+(x+2) = 2x, \qquad x\cdot(2x) = 1,$$
$$(2x+1)+x = 1, \qquad (2x+1)\cdot x = x+1,$$

и т.д.

Построение поля $\mathbb{F}_3^2$...

Заметим, что, например,

$$
\begin{aligned}
(x+1)^1 &= x+1, & (x+1)^5 &= 2x+2,\\
(x+1)^2 &= 2x, & (x+1)^6 &= x,\\
(x+1)^3 &= 2x+1, & (x+1)^7 &= x+2,\\
(x+1)^4 &= 2, & (x+1)^8 &= 1.
\end{aligned}
$$

Построение поля $\mathbb{F}_3^2$...

Заметим, что, например,

$$\begin{aligned}
(x+1)^1 &= x+1, & (x+1)^5 &= 2x+2,\\
(x+1)^2 &= 2x, & (x+1)^6 &= x,\\
(x+1)^3 &= 2x+1, & (x+1)^7 &= x+2,\\
(x+1)^4 &= 2, & (x+1)^8 &= 1.
\end{aligned}$$

Это значит, что $x+1$ — примитивный элемент поля $\mathbb{F}_3^2$ (а x — нет, поскольку $x^4 = 4 \equiv_3 1$).

Построение поля $\mathbb{F}_3^2$...

Заметим, что, например,

$$\begin{aligned}(x+1)^1 &= x+1, & (x+1)^5 &= 2x+2,\\ (x+1)^2 &= 2x, & (x+1)^6 &= x,\\ (x+1)^3 &= 2x+1, & (x+1)^7 &= x+2,\\ (x+1)^4 &= 2, & (x+1)^8 &= 1.\end{aligned}$$

Это значит, что $x+1$ — примитивный элемент поля $\mathbb{F}_3^2$ (а x — нет, поскольку $x^4 = 4 \equiv_3 1$).

Вопрос

Что будет, если при построении поля вместо x^2+1 взять другой неприводимый в $\mathbb{F}_3[x]$ многочлен?
Например, $2x^2+x+1$?

Построение поля $\mathbb{F}_3^2$...

Заметим, что, например,

$$\begin{aligned}(x+1)^1 &= x+1, & (x+1)^5 &= 2x+2,\\ (x+1)^2 &= 2x, & (x+1)^6 &= x,\\ (x+1)^3 &= 2x+1, & (x+1)^7 &= x+2,\\ (x+1)^4 &= 2, & (x+1)^8 &= 1.\end{aligned}$$

Это значит, что $x+1$ — примитивный элемент поля $\mathbb{F}_3^2$ (а x — нет, поскольку $x^4 = 4 \equiv_3 1$).

Вопрос

Что будет, если при построении поля вместо x^2+1 взять другой неприводимый в $\mathbb{F}_3[x]$ многочлен?
Например, $2x^2+x+1$?

Ответ: получится поле, изоморфное построенному.

Вычисления в конечном поле: пример

Задача. Опередить, является ли:
1) многочлен $a(x) = x^3 + 2x + 4 \in \mathbb{F}_5[x]$ — неприводимым?
2) элемент $4x^2 + 2$ — корнем $a(x)$ в фактор-кольце/поле $\mathbb{F}_5[x]/\big(x^3 + 2x + 4\big)$?

Вычисления в конечном поле: пример

Задача. Опередить, является ли:
1) многочлен $a(x) = x^3 + 2x + 4 \in \mathbb{F}_5[x]$ — неприводимым?
2) элемент $4x^2 + 2$ — корнем $a(x)$ в фактор-кольце/поле $\mathbb{F}_5[x]/\big(x^3 + 2x + 4\big)$?

Решение.
1. Перебором элементов $x \in GF(5) = \{0, 1, 2, 3, 4\}$ —

$$a(0) = 4,\ f(1) = 2,\ a(2) = 1,\ a(3) = 2,\ a(4) = 1$$

убеждаемся $a(x)$ — неприводимый многочлен
(а если бы это был многочлен 4-й степени?).
Следовательно, фактор-кольцо $F = \mathbb{F}_5[x]/\big(x^3 + 2x + 4\big)$
является полем и в нём $x^3 = -2x - 4 = 3x + 1$.

Вычисления в конечном поле: пример

Задача. Опередить, является ли:
1) многочлен $a(x) = x^3 + 2x + 4 \in \mathbb{F}_5[x]$ — неприводимым?
2) элемент $4x^2 + 2$ — корнем $a(x)$ в фактор-кольце/поле $\mathbb{F}_5[x]/\big(x^3 + 2x + 4\big)$?

Решение.
1. Перебором элементов $x \in GF(5) = \{0, 1, 2, 3, 4\}$ —

$$a(0) = 4,\ f(1) = 2,\ a(2) = 1,\ a(3) = 2,\ a(4) = 1$$

убеждаемся $a(x)$ — неприводимый многочлен
(а если бы это был многочлен 4-й степени?).
Следовательно, фактор-кольцо $F = \mathbb{F}_5[x]/\big(x^3 + 2x + 4\big)$
является полем и в нём $x^3 = -2x - 4 = 3x + 1$.

2. $a(4x^2 + 2) = \big(2(2x^2 + 2)\big)^3 + 4(2x^2 + 1) + 4 =$
$= 3(3x^6 + 2x^4 + x^2 + 1) + 3x^2 + 3 = 4x^6 + x^4 + x^2 + 1 =$
$= 4(3x+1)^2 + 3x^2 + x + x^2 + 1 = x^2 + 4x + 4 + 3x^2 + x + x^2 + 1 = 0.$

Как найти примитивные элементы поля $\mathbb{F}_p^n$?

$f(x)$ — примитивный элемент (генератор) группы $\mathbb{F}_p^{n*}$, если

1. $\big(f(x)\big)^{p^n-1} = 1$ и $\big(f(x)\big)^i \neq 1$ для $0 < i < p^n - 1$,
2. для любого многочлена $g(x) \in \mathbb{F}_p^{n*}$ найдётся степень i такая, что $g(x) = \big(f(x)\big)^i$, $i \in \{0, 1, \ldots, p^n - 1\}$.

Как найти примитивные элементы поля $\mathbb{F}_p^n$?

$f(x)$ — примитивный элемент (генератор) группы $\mathbb{F}_p^{n*}$, если

1. $\big(f(x)\big)^{p^n-1} = 1$ и $\big(f(x)\big)^i \neq 1$ для $0 < i < p^n - 1$,
2. для любого многочлена $g(x) \in \mathbb{F}_p^{n*}$ найдётся степень i такая, что $g(x) = \big(f(x)\big)^i$, $i \in \{0, 1, \ldots, p^n - 1\}$.

На основе известного: если α — примитивный элемент поля $GF(q)$, то любой другой примитивный элемент может быть получен как степень α^k, где k — целое взаимно простое с $q-1$ $\Rightarrow$ количество примитивных элементов поля $\mathbb{F}_p^n$ равно $\varphi(p^n - 1)$.

Как найти примитивные элементы поля $\mathbb{F}_p^n$?

$f(x)$ — примитивный элемент (генератор) группы $\mathbb{F}_p^{n*}$, если

1. $\big(f(x)\big)^{p^n-1} = 1$ и $\big(f(x)\big)^i \neq 1$ для $0 < i < p^n - 1$,
2. для любого многочлена $g(x) \in \mathbb{F}_p^{n*}$ найдётся степень i такая, что $g(x) = \big(f(x)\big)^i$, $i \in \{0, 1, \ldots, p^n - 1\}$.

На основе известного: если α — примитивный элемент поля $GF(q)$, то любой другой примитивный элемент может быть получен как степень α^k, где k — целое взаимно простое с $q-1$ $\Rightarrow$ количество примитивных элементов поля $\mathbb{F}_p^n$ равно $\varphi(p^n-1)$.

Например, в 9-элементном поле $\mathbb{F}_3^2$ имеется $\varphi(8) = 4$ примитивных элемента, образованных степенями $1,\ 3,\ 5,\ 7$ (числа, взаимно простые с 8) уже найденного генератора:

$$x+1,\ (x+1)^3 = 2x+1,\ (x+1)^5 = 2x+2,\ (x+1)^7 = x+2.$$

Я что-то не понимаю: неприводимые многочлены — это примитивные элементы?

Я что-то не понимаю: неприводимые многочлены — это примитивные элементы?

Ведь было: для поиска и тех, и других нет эффективных алгоритмов...

Я что-то не понимаю: неприводимые многочлены — это примитивные элементы?

Ведь было: для поиска и тех, и других нет эффективных алгоритмов...

- Неприводимые многочлены ищут в кольце многочленов $\mathbb{F}_p[x]$ над простым полем $\mathbb{F}_p$ — например, чтобы построить его расширение.

Я что-то не понимаю: неприводимые многочлены — это примитивные элементы?

Ведь было: для поиска и тех, и других нет эффективных алгоритмов...

- Неприводимые многочлены ищут в кольце многочленов $\mathbb{F}_p[x]$ над простым полем $\mathbb{F}_p$ — например, чтобы построить его расширение.
- Примитивные элементы ищут в мультипликативной группе поля $\mathbb{F}_p^n$ — например, чтобы иметь удобное представление ненулевых элементов поля через его степени.

Я что-то не понимаю: неприводимые многочлены — это примитивные элементы?

Ведь было: для поиска и тех, и других нет эффективных алгоритмов...

- Неприводимые многочлены ищут в кольце многочленов $\mathbb{F}_p[x]$ над простым полем $\mathbb{F}_p$ — например, чтобы построить его расширение.
- Примитивные элементы ищут в мультипликативной группе поля $\mathbb{F}_p^n$ — например, чтобы иметь удобное представление ненулевых элементов поля через его степени.

Замечание: в поле $GF\left(p^n\right)$ понятие «неприводимый многочлен» не имеет смысла: там любой многочлен делится на любой ненулевой.

Например, в $\mathbb{F}_3[x]/\left(x^2+1\right)$: $\dfrac{x+1}{2x+1} = x.$

Может ли приводимый многочлен быть примитивным элементом?

Может ли приводимый многочлен быть примитивным элементом?

1. Возьмём поле $\mathbb{F}_2 = \{0, 1\}$.
2. Возьмём неприводимый над $\mathbb{F}_2$ многочлен $x^3 + x + 1$.
3. Построим поле $F = \mathbb{F}_2[x]/(x^3 + x + 1) \cong \mathbb{F}_2^3$; оно содержит все полиномы из $\mathbb{F}_2[x]$ степени $\leqslant 2$.
4. Многочлен $P(x) = x^2 + x = x(x + 1)$ — приводим в любом кольце, в т.ч. — в $\mathbb{F}_2[x]$, и он принадлежит F.
5. Является ли $P(x)$ — примитивным элементом поля F?

Может ли приводимый многочлен быть примитивным элементом?

1. Возьмём поле $\mathbb{F}_2 = \{0, 1\}$.
2. Возьмём неприводимый над $\mathbb{F}_2$ многочлен $x^3 + x + 1$.
3. Построим поле $F = \mathbb{F}_2[x]/(x^3 + x + 1) \cong \mathbb{F}_2^3$; оно содержит все полиномы из $\mathbb{F}_2[x]$ степени $\leqslant 2$.
4. Многочлен $P(x) = x^2 + x = x(x + 1)$ — приводим в любом кольце, в т.ч. — в $\mathbb{F}_2[x]$, и он принадлежит F.
5. Является ли $P(x)$ — примитивным элементом поля F?

Мультипликативная группа поля F содержит $2^3 - 1 = 7$ элементов, это простое число $\Rightarrow$ в мультипликативная группе все $\varphi(7) = 6$ неединичных элеметов — генераторы $\Rightarrow$ ответ на оба вопроса — ДА!

Может ли приводимый многочлен быть примитивным элементом?...

Удостоверимся, что $\alpha = x^2 + x = x(x+1)$ — примитивный элемент поля $F = \mathbb{F}_2[x]/\big(x^3 + x + 1\big)$.
В F: $x^3 = x + 1$ и

$$
\begin{aligned}
\alpha &= x^2 + x, \\
\alpha^2 &= x^4 + x^2 = \cancel{x^2} + x + \cancel{x^2} = x, \\
\alpha^3 &= \alpha \cdot \alpha^2 = x^3 + x^2 = x^2 + x + 1, \\
\alpha^4 &= (\alpha^2)^2 = x^2, \\
\alpha^5 &= \alpha^2\alpha^3 = x^3 + x^2 + x = \cancel{x} + 1 + x^2 + \cancel{x} = x^2 + 1, \\
\alpha^6 &= x^4 + x^2 + 1 = x^2 + x + x^2 + 1 = x + 1, \\
\alpha^7 &= x^2(x^2 + x + 1) = x^4 + x^3 + x^2 = \cancel{x^2} + \cancel{x} + \cancel{x} + 1 + \cancel{x^2} = 1.
\end{aligned}
$$

Всегда ли неприводимый многочлен есть примитивный элемент?

Всегда ли неприводимый многочлен есть примитивный элемент?

1. Возьмём поле $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$.
2. Возьмём неприводимый над $\mathbb{F}_5$ многочлен $x^2 + x + 1$.
3. Построим поле $F = \mathbb{F}_5[x]/(x^2 + x + 1) \cong \mathbb{F}_5^2$; оно содержит только полиномы 0-й и 1-й степеней из $\mathbb{F}_5[x]$.
4. Все многочлены 1-й степени неприводимы, имеют вид $ax + b$ и их — 20 шт.
   Все ли они — примитивные элементы поля F?

Всегда ли неприводимый многочлен есть примитивный элемент?

1. Возьмём поле $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$.
2. Возьмём неприводимый над $\mathbb{F}_5$ многочлен $x^2 + x + 1$.
3. Построим поле $F = \mathbb{F}_5[x]/(x^2 + x + 1) \cong \mathbb{F}_5^2$; оно содержит только полиномы 0-й и 1-й степеней из $\mathbb{F}_5[x]$.
4. Все многочлены 1-й степени неприводимы, имеют вид $ax + b$ и их — 20 шт.
   Все ли они — примитивные элементы поля F?

Мультипликативная группа поля F содержит $5^2 - 1 = 24$ элемента из которых $\varphi(24) = 8$ примитивных $\Rightarrow$ не все многочлены 1-й степени — генераторы $\Rightarrow$
ответ на оба вопроса — НЕТ!

Всегда ли неприводимый многочлен есть примитивный элемент?...

Удостоверимся, что $\alpha = x$ **не есть** примитивный элемент поля $F = \mathbb{F}_5[x]/\left(x^2 + x + 1\right)$.

В F: $x^2 = -x - 1 = 4x + 4$ и

$$\begin{aligned} \alpha &= x \\ \alpha^2 &= 4x + 4, \\ \alpha^3 &= 4x^2 + 4x = 16x + 16 + 4x = 1. \end{aligned}$$

Интересный (и важный!) вопрос:

когда x есть примитивный элемент поля $\mathbb{F}_p[x]/(a(x))$?

Примитивные многочлены

Вопрос: когда корень x (сам неприводимый многочлен!) неприводимого над $\mathbb{F}_p$ многочлена $a(x)$ будет примитивным элементом поля $\mathbb{F}_p[x]/(a(x))$?

Примитивные многочлены

Вопрос: когда корень x (сам неприводимый многочлен!) неприводимого над $\mathbb{F}_p$ многочлена $a(x)$ будет примитивным элементом поля $\mathbb{F}_p[x]/(a(x))$?

Ответ: это будет если и только если $a(x)$ *примитивен* для x, т.е. $m = p^n - 1$ — наименьший показатель, при котором $a(x) \mid x^m - 1$.

Примитивные многочлены

Вопрос: когда корень x (сам неприводимый многочлен!) неприводимого над $\mathbb{F}_p$ многочлена $a(x)$ будет примитивным элементом поля $\mathbb{F}_p[x]/(a(x))$?

Ответ: это будет если и только если $a(x)$ *примитивен* для x, т.е. $m = p^n - 1$ — наименьший показатель, при котором $a(x) \mid x^m - 1$.

Пример

❶ Неприводимый над $\mathbb{F}_2$ многочлен $x^3 + x + 1$ примитивен: $x^{2^3-1} - 1 = x^7 + 1 = (x^3 + x + 1)(x^4 + x^2 + x + 1)$ и $x^t - 1 \not\vdots x^3 + x + 1$ ни при каком $1 \leqslant t < 7 = m$. Поэтому

$$\mathbb{F}_2^*[x]/\left(x^3 + x + 1\right) = \left\{ x^0 = 1, x^1, x^2, x^3 = x + 1, \right.$$
$$\left. x^4 = x^2 + x, x^5 = x^2 + x + 1, x^6 = x^2 + 1 \right\}.$$

Примитивные многочлены...

❷ Неприводимый над $\mathbb{F}_2$ многочлен $x^4+x^3+x^2+x+1$ не примитивен: он делит не только бином $x^{2^4-1}-1=x^{15}-1$, но и бином x^5-1:

$$x^5-1=x^5+1=(x^4+x^3+x^2+x+1)\cdot(x+1),$$

или, что тоже, $\deg x=5\neq 15$:

$$x^5=\underbrace{(x^4+x^3+x^2+x+1)\cdot(x+1)}_{=0}+1=1.$$

Примитивные многочлены: задача

Определить, является ли неприводимый многочлен $f(x) = x^6 + x^3 + 1 \in \mathbb{F}_2[x]$ *примитивным?*

Примитивные многочлены: задача

Определить, является ли неприводимый многочлен $f(x) = x^6 + x^3 + 1 \in \mathbb{F}_2[x]$ *примитивным?*

Решение

Мультипликативная группа поля $\mathbb{F}_2[x]/\left(x^6 + x^3 + 1\right)$ состоит из $2^6 - 1 = 63$ элементов.

Простые делители $63 = 3^2 \cdot 7$ суть 3 и 7 $\Rightarrow$ равенство $x^d = 1$ нужно проверить для $d \in \{\, 21, 9 \,\}$.

В рассматриваемом поле $x^6 = x^3 + 1$ и

$$x^9 = x^6 x^3 = (x^3 + 1)x^3 = x^6 + x^3 = \cancel{x^3} + 1 + \cancel{x^3} = 1.$$

Т.о. $\deg x = 9 \neq 63$ и многочлен $f(x)$ не примитивен.

Разделы

Алгоритм Евклида —

— применяют для нахождения НОД(a, b) натуральных a и b.

Наблюдение: общий делитель пары чисел (a, b), то остаётся им и для пары $(a - b, b)$ (считаем, что $a \geqslant b$).

Алгоритм Евклида —

— применяют для нахождения НОД(a, b) натуральных a и b.

Наблюдение: общий делитель пары чисел (a, b), то остаётся им и для пары $(a - b, b)$ (считаем, что $a \geqslant b$).

Отсюда:

- пары чисел (a, b) и $(a - kb, b)$ имеет одинаковые общие делители;

Алгоритм Евклида —

— применяют для нахождения НОД(a, b) натуральных a и b.

Наблюдение: общий делитель пары чисел (a, b), то остаётся им и для пары $(a - b, b)$ (считаем, что $a \geqslant b$).

Отсюда:

- пары чисел (a, b) и $(a - kb, b)$ имеет одинаковые общие делители;
- вместо $a - kb$ (для «ускорения») можно взять остаток r_0 от деления нацело a на b: $a = bq + r_0$, $q \in \mathbb{N}$, $0 \leqslant r_0 < b$;

Алгоритм Евклида —

— применяют для нахождения НОД(a, b) натуральных a и b.

Наблюдение: общий делитель пары чисел (a, b), то остаётся им и для пары $(a - b, b)$ (считаем, что $a \geqslant b$).

Отсюда:

- пары чисел (a, b) и $(a - kb, b)$ имеет одинаковые общие делители;
- вместо $a - kb$ (для «ускорения») можно взять остаток r_0 от деления нацело a на b: $a = bq + r_0$, $q \in \mathbb{N}$, $0 \leqslant r_0 < b$;
- затем, переставив числа в паре, можно повторить процедуру; она закончится, т.к. числа в паре уменьшаются, но остаются неотрицательными.

Алгоритм Евклида —

— применяют для нахождения НОД(a, b) натуральных a и b.

Наблюдение: общий делитель пары чисел (a, b), то остаётся им и для пары $(a - b, b)$ (считаем, что $a \geqslant b$).

Отсюда:

- пары чисел (a, b) и $(a - kb, b)$ имеет одинаковые общие делители;
- вместо $a - kb$ (для «ускорения») можно взять остаток r_0 от деления нацело a на b: $a = bq + r_0$, $q \in \mathbb{N}$, $0 \leqslant r_0 < b$;
- затем, переставив числа в паре, можно повторить процедуру; она закончится, т.к. числа в паре уменьшаются, но остаются неотрицательными.

В результате: за конечное число шагов образуется пара $(r_n, 0)$ и ясно, что НОД$(a, b) = r_n$. (НОД — англ. gcd)

Алгоритм Евклида —

— применяют для нахождения НОД(a, b) натуральных a и b.

Наблюдение: общий делитель пары чисел (a, b), то остаётся им и для пары $(a - b, b)$ (считаем, что $a \geqslant b$).

Отсюда:

- пары чисел (a, b) и $(a - kb, b)$ имеет одинаковые общие делители;
- вместо $a - kb$ (для «ускорения») можно взять остаток r_0 от деления нацело a на b: $a = bq + r_0$, $q \in \mathbb{N}$, $0 \leqslant r_0 < b$;
- затем, переставив числа в паре, можно повторить процедуру; она закончится, т.к. числа в паре уменьшаются, но остаются неотрицательными.

В результате: за конечное число шагов образуется пара $(r_n, 0)$ и ясно, что НОД$(a, b) = r_n$. (НОД — англ. gcd)
Данный алгоритм дважды описан в *Началах* Евклида, но не был им открыт (упоминается в *Топике* Аристотеля).

Алгоритм Евклида: общая схема $(a \geqslant b)$

НОД (a, b) $\boxed{=}$

Шаг (-2): $r_{-2} = a$ — полагаем для удобства;

Шаг (-1): $r_{-1} = b$ — полагаем для удобства;

Шаг 0: $r_{-2} = r_{-1}q_0 + r_0$ — делим r_{-2} на r_{-1}, остаток r_0;

Шаг 1: $r_{-1} = r_0 q_1 + r_1$ — делим r_{-1} на r_0, остаток r_1;

... *всегда делим с остатком бóльшее число на меньшее, оставляем меньшее (оно становится бóльшим) и остаток (он становится меньшим)*;

Шаг n: $r_{n-2} = r_{n-1}q_n + r_n$ — делим r_{n-2} на r_{n-1}, остаток r_n;

Шаг $n+1$: $r_{n-1} = r_n q_{n+1} + 0$ — деление нацело $\Rightarrow$ **останов**.

Всегда $r_{-2} \geqslant r_{-1} > r_0 > r_1 > \ldots > r_n \geqslant 1$. $\boxed{=} r_n$.

Алгоритм Евклида: пример

$$\underline{\text{НОД}\,(252, 105) = 21}$$

Алгоритм Евклида: пример

$\underline{\text{НОД}\,(252, 105) = 21}$

Шаг (-2): $r_{-2} = 252;$

Шаг (-1): $r_{-1} = 105 \Rightarrow (252, 105);$

Шаг 0: $252 = 105 \cdot 2 + 42 \Rightarrow (105, 42);$

Шаг 1: $105 = 42 \cdot 2 + 21 \Rightarrow (42, 21);$

Шаг 2: $42 = 21 \cdot 2 + 0 \Rightarrow (\mathbf{21}, 0).$

Алгоритм Евклида: пример

$\underline{\text{НОД}\,(252, 105) = 21}$

$$\begin{aligned}
&\text{Шаг } (-2): && r_{-2} = 252; && \\
&\text{Шаг } (-1): && r_{-1} = 105 && \Rightarrow (252, 105); \\
&\text{Шаг } 0: && 252 = 105 \cdot 2 + 42 && \Rightarrow (105, 42); \\
&\text{Шаг } 1: && 105 = 42 \cdot 2 + 21 && \Rightarrow (42, 21); \\
&\text{Шаг } 2: && 42 = 21 \cdot 2 + 0 && \Rightarrow (\mathbf{21}, 0).
\end{aligned}$$

$$\text{НОД}\,(a, b, c) = \text{НОД}\,(a, (\text{НОД}\,(b, c))$$

Интересно: если $a = F_{n+1}$, $b = F_n$ — соответствующие числа Фиббоначи, то остатки в алгоритме Евклида последовательно дадут значения $F_{n-1}, \ldots, F_2 = 1$.

Соотношение Безу (открыто за 106 лет до рождения Э.Безу)

Утверждение (соотношение Безу)

Для любых натуральных a, b *и* $d = НОД(a, b)$ *найдутся целые коэффициенты Безу* x, y *такие, что* $d = ax + by$.

Соотношение Безу (открыто за 106 лет до рождения Э.Безу)

Утверждение (соотношение Безу)

Для любых натуральных a, b *и* $d = НОД(a, b)$ *найдутся целые коэффициенты Безу* x, y *такие, что* $d = ax + by$.

Доказательство

Рассматриваем алгоритм Евклида с конца к началу: $d = r_n = r_{n-2} - r_{n-1}q_n$, *затем, подставляя сюда значение* $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$, *получаем*

$$d = -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2} = \alpha r_{n-3} + \beta r_{n-2}$$

для некоторых $\alpha, \beta \in \mathbb{Z}$ *и т.д.*

Соотношение Безу (открыто за 106 лет до рождения Э.Безу)

Утверждение (соотношение Безу)

Для любых натуральных a, b *и* $d = \text{НОД}(a, b)$ *найдутся целые коэффициенты Безу* x, y *такие, что* $d = ax + by$.

Доказательство

Рассматриваем алгоритм Евклида с конца к началу: $d = r_n = r_{n-2} - r_{n-1}q_n$, *затем, подставляя сюда значение* $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$, *получаем*

$$d = -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2} = \alpha r_{n-3} + \beta r_{n-2}$$

для некоторых $\alpha, \beta \in \mathbb{Z}$ *и т.д.*

Замечание Коэффициенты Безу определены неоднозначно:

$$\text{НОД}(12, 30) = 6 = 3 \cdot 12 + (-1) \cdot 30 = (-2) \cdot 12 + 1 \cdot 30.$$

Расширенный алгоритм Евклида —

— повторяет схему (простого) алгоритма Евклида, в котором на каждом шаге:

1. дополнительно вычисляются x_i и y_i по формулам

$$x_i = x_{i-2} - q_i x_{i-1}, \quad y_i = y_{i-2} - q_i y_{i-1}, \qquad i = 0, 1, \ldots;$$
$$x_{-2} = y_{-1} = 1, \quad x_{-1} = y_{-2} = 0;$$

2. справедливо соотношение

$$r_i = r_{i-2} - q_i r_{i-1} = (ax_{i-2} + by_{i-2}) - q_i(ax_{i-1} + by_{i-1}) =$$
$$= a(x_{i-2} - q_i x_{i-1}) + b(y_{i-2} - q_i y_{i-1}) = ax_i + by_i.$$

Расширенный алгоритм Евклида по двум натуральным числам a и b находит их натуральный НОД d и два целых x, y коэффициента Безу (таких, что $|x| < |b/d|$, $|y| < |a/d|$).

Расширенный алгоритм Евклида: пример

Задача. Найти натуральное d и целые x и y такие, что

$$d = \text{НОД}\,(252, 105) = 252x + 105y.$$

Решение. Имеем $x_i = x_{i-2} - q_i x_{i-1}$, $y_i = y_{i-2} - q_i y_{i-1}$.
Сведём все вычисления в таблицу:

шаг i	r_{i-2}	r_{i-1}	q_i	r_i	x_i	y_i
-2				252	1	0
-1				105	0	1
0	252	105	2	42	1	-2
1	105	42	2	21	-2	5
2	42	21	2	0		

Ответ: $d = 21$, $x = -2$, $y = 5$, т.е. $21 = 252 \cdot (-2) + 105 \cdot 5$.

Задача

В поле $\mathbb{Z}/(101)$ *решить уравнение* $4x = 1.$ $(*)$

Задача

В поле $\mathbb{Z}/(101)$ *решить уравнение* $4x = 1.$ $(*)$

Решение

1. $4x = 1 + k \cdot 101 = 102, 203, 304, \ldots;$ $x = 304/4 = 76.$
   Это решение перебором.

Задача

В поле $\mathbb{Z}/(101)$ *решить уравнение* $4x = 1.$ $(*)$

Решение

1. $4x = 1 + k \cdot 101 = 102, 203, 304, \ldots;$ $x = 304/4 = 76.$
   Это решение перебором.

2. Поскольку $101y \equiv_{101} 0$, вместо $(*)$ можно расширенным алгоритмом Евклида решать уравнение
   $$4x + 101y = 1\,.$$

Задача

В поле $\mathbb{Z}/(101)$ *решить уравнение* $4x = 1.$ $(*)$

Решение

1. $4x = 1 + k \cdot 101 = 102, 203, 304, \ldots;$ $x = 304/4 = 76.$
   Это решение перебором.

2. Поскольку $101y \equiv_{101} 0$, вместо $(*)$ можно расширенным алгоритмом Евклида решать уравнение
   $$4x + 101y = 1\,.$$
   В результате работы алгоритма: $4 \cdot 76 + 101 \cdot (-3) = 1.$

Аналогично решаются уравнения

$$ax = c \quad \text{и} \quad ax + by = c$$

(перед решением a, b и c надо поделить на их общий НОД).

Нахождение обратных элементов в расширениях полей $\mathbb{F}_p$

Алгоритм Евклида и его расширенная версия остаются справедливыми в любом евклидовом кольце, следовательно, и в любом поле Галуа.

Нахождение обратных элементов в расширениях полей $\mathbb{F}_p$

Алгоритм Евклида и его расширенная версия остаются справедливыми в любом евклидовом кольце, следовательно, и в любом поле Галуа.

Поэтому: обратный элемент $y(x)$ для некоторого многочлена $b(x)$ в поле $F = \mathbb{F}_p[x]/(a(x))$ определяется соотношением

$$b(x) \cdot y(x) = 1 \quad \Leftrightarrow \quad a(x) \cdot \chi(x) + b(x) \cdot y(x) = 1\,,$$

которое может быть решено расширенным алгоритмом Евклида для пары многочленов $(a(x), b(x))$ в поле F.

Решение данных уравнений существует всегда: т.к. $a(x)$ — неприводимый многочлен и $\deg b(x) < \deg a(x)$, то НОД $(a(x), b(x)) = 1$.

Пример: найти $(x^2+x+3)^{-1}$ в поле $\mathbb{F}_7[x]/\left(x^4+x^3+x^2+3\right)$

Пример: найти $(x^2+x+3)^{-1}$ в поле $\mathbb{F}_7[x]/\left(x^4+x^3+x^2+3\right)$

Применяя расширенный алгоритм Евклида, решим уравнение

$$(x^4+x^3+x^2+3)\chi(x) + (x^2+x+3)y(x) = 1 \qquad (*)$$

Пример: найти $(x^2+x+3)^{-1}$ в поле $\mathbb{F}_7[x]/(x^4+x^3+x^2+3)$

Применяя расширенный алгоритм Евклида, решим уравнение

$$(x^4+x^3+x^2+3)\chi(x) + (x^2+x+3)y(x) = 1 \qquad (*)$$

Шаг 0: $r_{-2}(x) = x^4+x^3+x^2+3,$
$r_{-1}(x) = x^2+x+3,$
$y_{-2}(x) = 0,$
$y_{-1}(x) = 1$ — задание начальных значений.

Шаг 1: $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x),$
$q_0(x) = x^2+5,$
$r_0(x) = 2x+2,$
$y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x) = -x^2-5.$

Шаг 2: $r_{-1}(x) = r_0(x)q_1(x) + r_1(x),$
$q_1(x) = 4x,$
$r_1(x) = 3, \quad \deg r_1(x) = 0$
$y_1(x) = y_{-1}(x) - y_0(x)q_1(x) = 1 + 4x(x^2+5) =$
$= 4x^3+6x+1.$

Пример... $\mathbb{F}_7^4: \ (x^4+x^3+x^2+3)\chi(x)+b(x)(x^2+x+3) = 1 \ \ (*)$

Алгоритм заканчивает свою работу на шаге 2, т.к. $r_1(x) = 3$ и $\deg r_1(x) = \deg 1 = 0$ (1 — многочлен в правой части $(*)$).

Пример... $\mathbb{F}_7^4$: $(x^4+x^3+x^2+3)\chi(x)+b(x)(x^2+x+3) = 1 \quad (*)$

Алгоритм заканчивает свою работу на шаге 2, т.к. $r_1(x) = 3$ и $\deg r_1(x) = \deg 1 = 0$ (1 — многочлен в правой части $(*)$).

Замечание: при итерациях алгоритма нет необходимости вычислять $\chi_i(x)$ — коэффициент при $x^4+x^3+x^2+3$, — т.к. нас интересует только $y_i(x)$ — коэффициент при x^2+x+3.

Остаток $r_1(x) = 3$, отличается от 1 на множитель-константу.

Пример... $\mathbb{F}_7^4$: $(x^4+x^3+x^2+3)\chi(x)+b(x)(x^2+x+3) = 1 \quad (*)$

Алгоритм заканчивает свою работу на шаге 2, т.к. $r_1(x) = 3$ и $\deg r_1(x) = \deg 1 = 0$ (1 — многочлен в правой части $(*)$).

Замечание: при итерациях алгоритма нет необходимости вычислять $\chi_i(x)$ — коэффициент при $x^4+x^3+x^2+3$, — т.к. нас интересует только $y_i(x)$ — коэффициент при x^2+x+3.

Остаток $r_1(x) = 3$, отличается от 1 на множитель-константу.

Чтобы получить решение уравнения $(*)$ вычисляем элемент $3^{-1} \equiv_7 5$ и домножаем на него y_1:

$$5y_1(x) = 5(4x^3+6x+1) \equiv_7 6x^3+2x+5.$$

Ответ: в поле $\mathbb{F}_7[x]/\left(x^4+x^3+x^2+3\right)$ имеем

$$(x^2+x+3)^{-1} = 6x^3+2x+5.$$

Разделы

Векторное пространство: определение

Определение

Абстрактным векторным пространством над полем $\Bbbk = \{1, \alpha, \beta, \dots\}$ называется алгебраическая система $\mathcal{V} = \langle V, \Bbbk; +, \cdot \rangle$, где

- $V = \{0, v, \dots\}$ — произвольное множество,
- $+$ — бинарная операция сложения над V: $V \times V \overset{+}{\to} V$,
- $\cdot$ — бинарная операция умножения элемента («числа») из $\Bbbk$ на элемент («вектор») из V: $\Bbbk \times V \overset{\cdot}{\to} V$,

Векторное пространство: определение

Определение

Абстрактным векторным пространством над полем $\Bbbk = \{1, \alpha, \beta, \dots\}$ называется алгебраическая система $\mathcal{V} = \langle V, \Bbbk; +, \cdot \rangle$, где

- $V = \{0, v, \dots\}$ — произвольное множество,
- $+$ — бинарная операция сложения над V: $V \times V \xrightarrow{+} V$,
- $\cdot$ — бинарная операция умножения элемента («числа») из $\Bbbk$ на элемент («вектор») из V: $\Bbbk \times V \xrightarrow{\cdot} V$,

причём операции $+$ и $\cdot$ удовлетворяют следующим аксиомам:

L1: V — коммутативная группа по сложению, 0 — её нейтральный элемент.

L2: $\alpha \cdot (v_1 + v_2) = \alpha \cdot v_1 + \alpha \cdot v_2$, $(\alpha_1 + \alpha_2) \cdot v = \alpha_1 \cdot v + \alpha_2 \cdot v$, (дистрибутивность $\cdot$ относительно $+$),

L3: $\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v$ (композиция умножений на два элемента поля совпадает с умножением их произведение, «ассоциативность» операций умножения поля и $\cdot$),

L4: $1 \cdot v = v$ (унитальность).

Координатное пространство

Пример

Пусть $V = \Bbbk^n$ — множество конечных последовательностей длины n элементов поля $\Bbbk$.
'Сложение' и 'умножение на число (из $\Bbbk$)' элементов из V определяются покомпонентно.

Получившаяся структура — векторное пространство.
Его называют *n-мерным координатным пространством* над полем $\Bbbk$.

Дистрибутивность относительно вычитания: $(\alpha - \beta) \cdot v = \alpha \cdot v - \beta \cdot v$:

$$(\alpha - \beta) \cdot v + \beta \cdot v = (\alpha - \beta + \beta) \cdot v = \alpha \cdot v$$

Отсюда получаем, что

- $0 \cdot v = 0$, так как $0 \cdot v = (1 - 1) \cdot v = v - v = 0$
- и $-v = (-1) \cdot v$, так как

$$v + (-1) \cdot v = 1 \cdot v + (-1) \cdot v = (1 - 1) \cdot v = 0 \cdot v = 0.$$

Применение векторной алгебры к изучению конечных полей

Лемма

Поле $\Bbbk$ *характеристики* $p > 0$ *есть векторное пространство над* $\mathbb{F}_p$.

Применение векторной алгебры к изучению конечных полей

Лемма

Поле $\Bbbk$ характеристики $p > 0$ есть векторное пространство над $\mathbb{F}_p$.

Доказательство

сложение — *наследуется операция сложения в поле $\Bbbk$;*

умножение — *поскольку*

$$\mathbb{F}_p \cong F = \{0, 1, 1+1, \ldots, \overbrace{1+\ldots+1}^{p-1}\} \subseteq \Bbbk,$$

то при умножении «числа» из поля $\mathbb{F}_p$ можно заменять на соответствующие элементы из поля F;

аксиомы векторного пространства — *выполняются в силу свойств арифметических операций в поле $\Bbbk$.*

Применение векторной алгебры к изучению конечных полей

Лемма

Поле $\Bbbk$ характеристики $p > 0$ есть векторное пространство над $\mathbb{F}_p$.

Доказательство

сложение — *наследуется операция сложения в поле $\Bbbk$;*

умножение — *поскольку*

$$\mathbb{F}_p \cong F = \{0, 1, 1+1, \ldots, \overbrace{1+\ldots+1}^{p-1}\} \subseteq \Bbbk,$$

то при умножении «числа» из поля $\mathbb{F}_p$ можно заменять на соответствующие элементы из поля F;

аксиомы векторного пространства — *выполняются в силу свойств арифметических операций в поле $\Bbbk$.*

Следствие

Поле Галуа как векторное пространство состоит из p^n элементов.

Поля Галуа как кольца вычетов или векторные пространства

Поле $\mathbb{F}_p^n$ есть конечная АС с элементами-многочленами

$$M_n(x) = \left\{ a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \right\} \subset \mathbb{F}_p[x],$$

которую можно рассматривать как

- фактор-кольцо вычетов по идеалу некоторого неприводимого многочлена $f(x)$ степени n над полем $\mathbb{F}_p$:

$$\mathbb{F}_p^n \cong \left\langle \mathbb{F}_p[x]/(f(x)) \,;\, +_p,\, \cdot_p \right\rangle$$

  или как

- n-мерное координатное пространство над полем $\mathbb{F}_p$:

$$\mathbb{F}_p^n \cong \left\langle M_n(x),\, \mathbb{F}_p;\, +_p,\, \cdot_p \right\rangle.$$

Базис в $\mathbb{F}_p^n$

Теорема

Элементы $\{1\}, \{x\}, \ldots, \{x^{n-1}\}$ *образуют базис* $\mathbb{F}_p^n$.

Базис в $\mathbb{F}_p^n$

Теорема

Элементы $\{1\}, \{x\}, \ldots, \{x^{n-1}\}$ *образуют базис* $\mathbb{F}_p^n$.

Доказательство

1. Любой элемент $\mathbb{F}_p^n$ *представим в виде линейной комбинации указанных векторов:*

$$\{a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}\} = \\ = a_0\{1\} + a_1\{x\} + \ldots + a_{n-1}\{x^{n-1}\}.$$

2. Обратно, пусть $g(x) = b_0\{1\} + b_1\{x\} + \ldots + b_{n-1}\{x^{n-1}\} = 0$. *Это означает, что многочлен* $g(x)$ *степени* $n-1$ *делится на некоторый многочлен* n*-й степени, что возможно лишь при* $b_0 = b_1 = \ldots = b_{n-1} = 0$, *т.е. система* $\{1\}, \{x\}, \ldots, \{x^{n-1}\}$ *линейно независима*.

$\mathbb{C}$ — расширение поля $\mathbb{R}$

Замечание. Построение поля с помощью вычетов по модулю некоторого неприводимого многочлена и аналоги доказанных теорем справедливы не только в случае конечных полей.

$\mathbb{C}$ — расширение поля $\mathbb{R}$

Замечание. Построение поля с помощью вычетов по модулю некоторого неприводимого многочлена и аналоги доказанных теорем справедливы не только в случае конечных полей.

Например:

1. рассмотрим поле действительных чисел $\mathbb{R}$ и кольцо многочленов $\mathbb{R}[x]$ над ним;
2. в $\mathbb{R}[x]$ возьмём неприводимый многочлен x^2+1;
3. построим поле F как фактор-кольцо: $F = \mathbb{R}[x]/\big(x^2+1\big)$;
4. F также и векторное пространство над $\mathbb{R}$; его базис — $\{\{1\},\{x\}\}$ и каждый его элемент $z \in F$ можно представить в виде $z = a\{1\} + b\{x\},\ a,b \in \mathbb{R}$;
5. поле F изоморфно полю комплексных чисел
$$\mathbb{C} = \{\, a+ib \mid a,b \in \mathbb{R},\ i^2 = -1 \,\},$$
изоморфизм задаётся соответствием $\{1\} \mapsto 1,\ \{x\} \mapsto i$.

Подполя $\mathbb{F}_p^n$

Лемма

Поле $\mathbb{F}_p^n$ *содержит подполе* $\mathbb{F}_p^k$ *iff* $k \mid n$.

Подполя $\mathbb{F}_p^n$

Лемма

Поле $\mathbb{F}_p^n$ содержит подполе $\mathbb{F}_p^k$ iff $k \mid n$.

Доказательство

Если поле $\Bbbk_1$ содержится в поле ($\Bbbk_1 \subset \Bbbk_2$), то элементы $\Bbbk_2$ можно умножать на элементы из $\Bbbk_1$, а результаты складывать. Поэтому поле $\Bbbk_2$ является векторным пространством над полем $\Bbbk_1$ некоторой размерности d — значит, в нём $|\Bbbk_1|^d$ элементов. Наш случай: $p^n = (p^k)^d$, что и означает $k \mid n$.

Обратное следует из существования и единственности (с точностью до изоморфизма) полей Галуа.

Ясно, что $\mathbb{F}_p$ — всегда подполе $\mathbb{F}_p^n$ (случай $k = 1$).

Подполя $\mathbb{F}_p^n$

Лемма

Поле $\mathbb{F}_p^n$ содержит подполе $\mathbb{F}_p^k$ iff $k \mid n$.

Доказательство

Если поле $\Bbbk_1$ содержится в поле ($\Bbbk_1 \subset \Bbbk_2$), то элементы $\Bbbk_2$ можно умножать на элементы из $\Bbbk_1$, а результаты складывать. Поэтому поле $\Bbbk_2$ является векторным пространством над полем $\Bbbk_1$ некоторой размерности d — значит, в нём $|\Bbbk_1|^d$ элементов. Наш случай: $p^n = (p^k)^d$, что и означает $k \mid n$.

Обратное следует из существования и единственности (с точностью до изоморфизма) полей Галуа.

Ясно, что $\mathbb{F}_p$ — всегда подполе $\mathbb{F}_p^n$ (случай $k = 1$).

Упражнение: перечислите все подполя поля $GF\left(2^{30}\right)$.

Представление элементов конечного поля: резюме

Наиболее употребимы два представления элементов конечного поля $F = \mathbb{F}_p[x]/(a(x)) \cong \mathbb{F}_p^n$ (полином $a(x)$ неприводим, $\deg a(x) = n$):

векторное — каждый элемент записывается как вектор в базисе $x^0 = 1,\ x^1,\ x^2,\ \ldots,\ x^{n-1}$.

степенное — каждый элемент записывается как степень α генератора мультипликативной группы F.

Представление элементов конечного поля: резюме

Наиболее употребимы два представления элементов конечного поля $F = \mathbb{F}_p[x]/(a(x)) \cong \mathbb{F}_p^n$ (полином $a(x)$ неприводим, $\deg a(x) = n$):

векторное — каждый элемент записывается как вектор в базисе $x^0 = 1,\ x^1,\ x^2,\ \ldots,\ x^{n-1}$.

степенное — каждый элемент записывается как степень α генератора мультипликативной группы F.

Замечание: переход от степенного представления к векторному достаточно прост, а обратный переход — очень сложен (связан с вычислением *дискретного логарифма* $\alpha^x = b(\alpha) \in F$).

На сложности этой задачи базируются методы криптографии с отрытым ключом. Известны не более, чем субэкспоненциальные алгоритмы её решения.

Разделы

Минимальный многочлен

Рассмотрим элемент β поля $\mathbb{F}_p^n$ и будем интересоваться многочленами, для которых он является корнем.

Определение

Многочлен $m_\beta(x) \in \mathbb{F}_p[x]$ называется *минимальным многочленом (м.м.)* или *минимальной функцией* для $\beta \in \mathbb{F}_p^n$, если это нормированный многочлен минимальной степени, для которого β является корнем.

Другими словами, должны выполняться три условия:

1. $m_\beta(\beta) = 0$;
2. $\forall\, f(x) \in \mathbb{F}_p[x] : \deg f(x) < \deg m_\beta(x) \Rightarrow f(\beta) \neq 0$;
3. коэффициент при старшей степени в $m_\beta(x)$ равен 1.

Почти очевидно, что м.м. — неприводимый (докажем после).

Минимальный многочлен из неприводимого

Рассмотрим поле $\mathbb{F}_p^n = \mathbb{F}_p[x]/(a(x))$, порождаемое неприводимым многочленом $a(x) = a_0 + a_1 x + \ldots + a_n x^n$ и убедимся, что многочлен $a_n^{-1} a(x)$ — минимальный для элемента $\overline{x} = (0, 1, 0, \ldots, 0) \in \mathbb{F}_p^n$.

Минимальный многочлен из неприводимого

Рассмотрим поле $\mathbb{F}_p^n = \mathbb{F}_p[x]/(a(x))$, порождаемое неприводимым многочленом $a(x) = a_0 + a_1 x + \ldots + a_n x^n$ и убедимся, что многочлен $a_n^{-1} a(x)$ — минимальный для элемента $\overline{x} = (0, 1, 0, \ldots, 0) \in \mathbb{F}_p^n$.

Действительно, с одной стороны —

$$a_0\overline{1} + a_1\overline{x} + \ldots + a_n\overline{x}^n = \overline{a_0 + a_1 x + \ldots + a_n x^n} = 0,$$

т.е. $\overline{x}$ — корень $a(x)$, а значит и $a_n^{-1} a(x)$.

С другой, пусть $b(x) = b_0\overline{1} + b_1\overline{x} + \ldots + b_{n-1}\overline{x}^{n-1} = 0$.
Но тогда $b_0\overline{1} + b_1\overline{x} + \ldots + b_{n-1}\overline{x^{n-1}} = 0$, т.е. имеем линейную зависимость между элементами $\left\{ \overline{1}, \overline{x}, \ldots, \overline{x^{n-1}} \right\}$ — базиса поля $\mathbb{F}_p^n$ как векторного пространства над $\mathbb{F}_p$, откуда $b_0 = b_1 = \ldots = b_{n-1} = 0$.

Минимальный многочлен из неприводимого

Рассмотрим поле $\mathbb{F}_p^n = \mathbb{F}_p[x]/(a(x))$, порождаемое неприводимым многочленом $a(x) = a_0 + a_1 x + \ldots + a_n x^n$ и убедимся, что многочлен $a_n^{-1} a(x)$ — минимальный для элемента $\overline{x} = (0, 1, 0, \ldots, 0) \in \mathbb{F}_p^n$.

Действительно, с одной стороны —

$$a_0\overline{1} + a_1\overline{x} + \ldots + a_n\overline{x}^n = \overline{a_0 + a_1 x + \ldots + a_n x^n} = 0,$$

т.е. $\overline{x}$ — корень $a(x)$, а значит и $a_n^{-1} a(x)$.

С другой, пусть $b(x) = b_0\overline{1} + b_1\overline{x} + \ldots + b_{n-1}\overline{x}^{n-1} = 0$.
Но тогда $b_0\overline{1} + b_1\overline{x} + \ldots + b_{n-1}\overline{x^{n-1}} = 0$, т.е. имеем линейную зависимость между элементами $\left\{ \overline{1}, \overline{x}, \ldots, \overline{x^{n-1}} \right\}$ — базиса поля $\mathbb{F}_p^n$ как векторного пространства над $\mathbb{F}_p$, откуда $b_0 = b_1 = \ldots = b_{n-1} = 0$.

$$\overline{x^2} = \overline{x}^2 = (0, 0, 1, 0, \ldots, 0), \quad \ldots, \quad \overline{x^{n-1}} = (0, \ldots, 0, 1)$$

Кстати, что такое $\overline{x}$?

Кстати, что такое $\overline{x}$?

Рассматриваем поле $\mathbb{F}_p^n = \mathbb{F}_p[x]/a(x)$, где $a(x) = a_0 + a_1 x + \ldots + a_n x^n$ — неприводимый многочлен, т.е. в этом поле

$$a(x) = 0 \Leftrightarrow x^n = {a_n}^{-1}\left(-a_0 - a_1 x - \ldots - a_{n-1}x^{n-1}\right).$$

Кстати, что такое $\overline{x}$?

Рассматриваем поле $\mathbb{F}_p^n = \mathbb{F}_p[x]/a(x)$, где
$a(x) = a_0 + a_1 x + \ldots + a_n x^n$ — неприводимый многочлен,
т.е. в этом поле

$$a(x) = 0 \Leftrightarrow x^n = {a_n}^{-1}\left(-a_0 - a_1 x - \ldots - a_{n-1}x^{n-1}\right).$$

1. $\overline{x} = \{ f(x) \in \mathbb{F}_p[x] \mid f(x) = q(x)a(x) + x,\ q(x) \in \mathbb{F}_p[x] \}.$

2. $\mathbb{F}_p^n =$
$= \left\{ f(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1} \mid b_0, b_1, \ldots, b_{n-1} \in \mathbb{F}_p \right\} =$
$= \{ (b_0, b_1, \ldots, b_{n-1}) \mid b_0, b_1, \ldots, b_{n-1} \in \mathbb{F}_p \}$

$\overline{x} = \{ (0, b_1, 0, \ldots, 0) \mid b_1 \in \mathbb{F}_p \}.$

В дальнейшем, как принято, вместо $\overline{x}$ часто пишем просто x.

Являются ли минимальные многочлены примитивными?

Являются ли минимальные многочлены примитивными?

Примеры из предыдущего.

1. $a(x) = x^3 + x + 1$ неприводим в $\mathbb{F}_2[x]$, следовательно:
   - $F = \mathbb{F}_2[x]/(a(x))$ — поле;
   - $a(x)$ — минимальный многочлен для x, т.к. «работаем» в $\mathbb{F}_2$, где $1^{-1} = 1$.

Примитивен ли $a(x)$?

Имеем в $F \cong GF(2^3)$: $a(x) \not| x^t - 1$ при $t = 3, 4, 5, 6$
(делимость $x^7 - 1$ на $a(x)$ всегда будет иметь место:
$x^7 + 1 = (x^3 + x + 1)(x^4 + x^2 + x + 1)$).

Это означает, что $a(x)$ — примитивный многочлен и
x — примитивный элемент поля F (генератор F^*, $\deg x = 7$).

Являются ли минимальные многочлены примитивными...

❷ $a(x) = x^4 + x^3 + x^2 + x + 1$ неприводим в $\mathbb{F}_2[x]$, следовательно:

- $F = \mathbb{F}_2[x]/(a(x))$ — поле;
- $a(x)$ — минимальный многочлен для x.

Примитивен ли $a(x)$?

Имеем в $F \cong GF(2^4)$:

$$a(x) \mid x^5 - 1 : \; x^5 + 1 = (x^4 + x^3 + x^2 + x + 1)(x + 1).$$

Это означает, что $a(x)$ — не есть примитивный многочлен и x — не генератор F^*, т.к. $\deg x = 5 \neq 15$.

Другое определение: минимальный многочлен примитивного элемента поля называется *примитивным многочленом*.

Свойства минимальных многочленов

Утверждение

Минимальные многочлены неприводимы.

Свойства минимальных многочленов

Утверждение

Минимальные многочлены неприводимы.

Доказательство

Пусть $m_\beta(x)$ *— м.м. для* β *и* $m_\beta(x) = m_1(x)m_2(x)$.
Тогда

$$m_\beta(\beta) = 0 \Rightarrow \left[\begin{array}{l} m_1(\beta) = 0 \\ m_2(\beta) = 0 \end{array} \right. ,$$

но $\deg m_1 < \deg m$ *и* $\deg m_2 < \deg m \Rightarrow \beta$ *не может быть корнем ни* $m_1(x)$, *ни* $m_2(x)$.

Свойства минимальных многочленов...

Утверждение

Пусть в некотором поле Галуа $m_\beta(x)$ *— м.м. для элемента* β*, а* $f(x)$ *— многочлен такой, что* $f(\beta) = 0$*.*
Тогда $f(x)$ *делится на* $m_\beta(x)$*.*

Свойства минимальных многочленов...

Утверждение

Пусть в некотором поле Галуа $m_\beta(x)$ *— м.м. для элемента* β*, а* $f(x)$ *— многочлен такой, что* $f(\beta) = 0$.
Тогда $f(x)$ *делится на* $m_\beta(x)$.

Доказательство

Разделим $f(x)$ *на* $m_\beta(x)$ *с остатком:*

$$f(x) = u(x)m_\beta(x) + v(x), \quad \deg v < \deg m.$$

Подставляя в это равенство β*, получаем*

$$0 = f(\beta) = u(\beta)\underbrace{m_\beta(\beta)}_{=0} + v(\beta) = v(\beta),$$

т.е. β *— корень* $v(x)$*, что противоречит минимальности* $m_\beta(x)$.

Свойства минимальных многочленов...

Следствие

Для каждого элемента поля существует не более одного м.м.

Свойства минимальных многочленов...

Следствие

Для каждого элемента поля существует не более одного м.м.

Доказательство

Пусть минимальных многочленов два.
Они взаимно делят друг друга, а значит, различаются на обратимый множитель-константу.
Поскольку минимальный многочлен нормирован, эта константа равна 1, т.е. данные многочлены совпадают.

Свойства минимальных многочленов...

Утверждение

Для каждого элемента β поля $\mathbb{F}_p^n$ существует (единственный) м.м. и его степень не превосходит n.

Свойства минимальных многочленов...

Утверждение

Для каждого элемента β *поля* $\mathbb{F}_p^n$ *существует (единственный) м.м. и его степень не превосходит* n.

Доказательство

Рассмотрим следующие элементы поля $\mathbb{F}_p^n$: $1, \beta, \beta^2, \ldots, \beta^n$ — *их* $n+1$ *штука, а размерность* $\mathbb{F}_p^n$ *как векторного пространства равна* n $\Rightarrow$ *эти элементы линейно зависимы, т.е. существуют такие не все равные* 0 *коэффициенты* $c_0, \ldots, c_n$, *что*

$$c_0 + c_1\beta + \ldots + c_n\beta^n = 0,$$

$\Rightarrow$ β — *корень многочлена* $f(x) = c_0 + c_1x + \ldots + c_nx^n$.

Минимальным многочленом для β *будет некоторый нормированный неприводимый делитель* $f(x)$ *(т.е.* $f(x) \in \mathbb{F}_p^n$*).*

Многочлены над конечным полем: свойства

Теорема

Любой ненулевой элемент поля $\mathbb{F}_p^n$ *является корнем многочлена* $x^{p^n-1}-1$, *т.е.*

$$x^{p^n-1}-1 = (x-\beta_1)\cdot\ldots\cdot(x-\beta_{p^n-1}),$$

где $\left\{\beta_1,\ldots,\beta_{p^n-1}\right\} = \mathbb{F}_p^{n*} = \mathbb{F}_p^n \setminus \{0\}$.

Многочлены над конечным полем: свойства

Теорема

Любой ненулевой элемент поля $\mathbb{F}_p^n$ *является корнем многочлена* $x^{p^n-1}-1$, *т.е.*

$$x^{p^n-1}-1 = (x-\beta_1)\cdot\ldots\cdot(x-\beta_{p^n-1}),$$

где $\{\beta_1,\ldots,\beta_{p^n-1}\} = \mathbb{F}_p^{n*} = \mathbb{F}_p^n \setminus \{0\}$.

Доказательство

$\mathbb{F}_p^{n*}$ *— циклическая группа по умножению порядка* p^n-1. *Порядок* $\deg\alpha$ *любого элемента* $\alpha \in \mathbb{F}_p^{n*}$ *(т.е. порядок циклической подгруппы* $\langle\alpha\rangle$*) по теореме Лагранжа делит порядок группы.*

Поэтому $p^n-1 = q\cdot\deg\alpha$, $\alpha^{\deg\alpha} = 1$ *и*

$$\alpha^{p^n-1}-1 = \alpha^{q\deg\alpha}-1 = (\alpha^{\deg\alpha})^q-1 = 1^q-1 = 0.$$

Многочлены над конечным полем: свойства...

Следствие (теорема Ферма)

Все элементы поля $\mathbb{F}_p^n$, *не исключая нуля, являются корнями многочлена* $x^{p^n} - x$.

Многочлены над конечным полем: свойства...

Следствие (теорема Ферма)

Все элементы поля $\mathbb{F}_p^n$, не исключая нуля, являются корнями многочлена $x^{p^n} - x$.

Доказательство

Вынесем x за скобку:

$$x^{p^n} - x = x\left(x^{p^n-1} - 1\right).$$

У второго сомножителя корнями будут все ненулевые элементы, а у первого — 0.

Многочлены над конечным полем: свойства...

Теорема

В кольце многочленов над конечным полем

$$(x^n - 1) \vdots (x^m - 1) \Leftrightarrow n \vdots m.$$

Многочлены над конечным полем: свойства...

Теорема

В кольце многочленов над конечным полем

$$(x^n - 1) \vdots (x^m - 1) \Leftrightarrow n \vdots m.$$

Доказательство

- *Пусть* $n = mk$. *Сделаем замену* $x^m = y$, *тогда* $x^n - 1 = y^k - 1$ *и* $x^m - 1 = y - 1$. *Делимость очевидна.*

Многочлены над конечным полем: свойства...

Теорема

В кольце многочленов над конечным полем

$$(x^n - 1) \vdots (x^m - 1) \Leftrightarrow n \vdots m.$$

Доказательство

- *Пусть* $n = mk$. *Сделаем замену* $x^m = y$, *тогда* $x^n - 1 = y^k - 1$ *и* $x^m - 1 = y - 1$. *Делимость очевидна.*
- *Предположим, что* $n \not\vdots m$, *т.е.* $n = km + r$, $0 < r < m$, *тогда*

$$x^n - 1 = \frac{x^r(x^{mk} - 1)(x^m - 1)}{x^m - 1} + x^r - 1 =$$

$$= \frac{x^r(x^{mk} - 1)}{x^m - 1}(x^m - 1) + x^r - 1.$$

Многочлены над конечным полем: свойства...

Последнее выражение задает результат деления $x^n - 1$ *на* $x^m - 1$ *с остатком, поскольку* $x^{mk} - 1$ *делится на* $x^m - 1$ *по доказанному выше.*
Остаток $x^r - 1 \neq 0$ *в силу сделанных предположений.*
$\therefore$ $x^n - 1$ *не делится на* $x^m - 1$.

Многочлены над конечным полем: свойства...

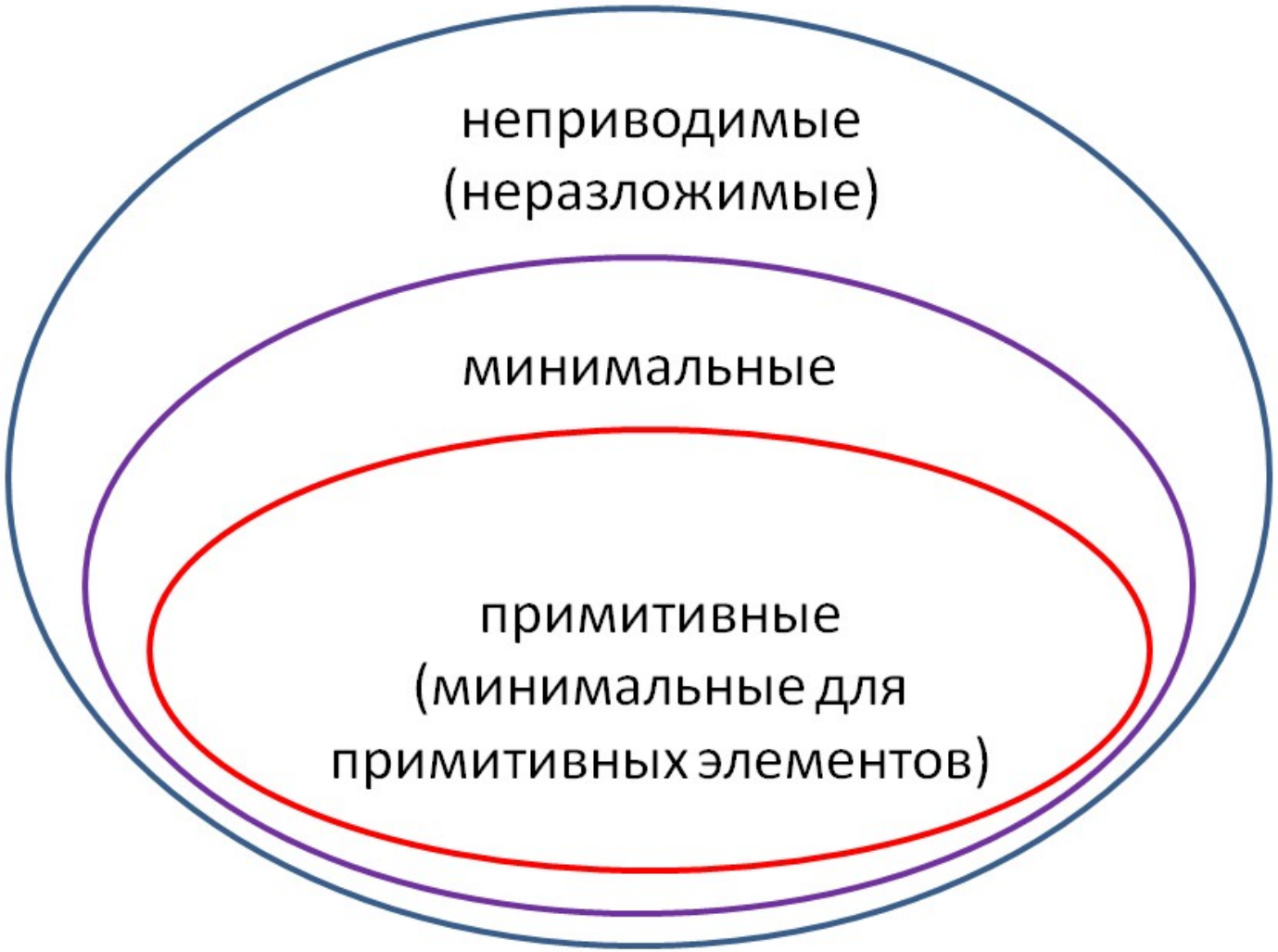
Последнее выражение задает результат деления $x^n - 1$ *на* $x^m - 1$ *с остатком, поскольку* $x^{mk} - 1$ *делится на* $x^m - 1$ *по доказанному выше.*
Остаток $x^r - 1 \neq 0$ *в силу сделанных предположений.*
$\therefore$ $x^n - 1$ *не делится на* $x^m - 1$.

Теорема даёт возможность раскладывать многочлены $x^n - 1$ при составных n.
Например, разложим $x^{15} + 1$ в $\mathbb{F}_2[x]$ (где $-1 = +1$):

$$x^{15} + 1 = (x^3 + 1)(x^{12} + x^9 + x^6 + x^3 + 1),$$
$$x^{15} + 1 = (x^5 + 1)(x^{10} + x^5 + 1).$$

Возможность раскладывать многочлены специального вида на неприводимые даёт следующая теорема.

Многочлены:


неприводимые
(неразложимые)
минимальные
примитивные
(минимальные для
примитивных элементов)

Разложение многочленов на неприводимые

Теорема

Все неприводимые многочлены n-й степени из $\mathbb{F}_p[x]$ делят многочлен $x^{p^n} - x$.

Разложение многочленов на неприводимые

Теорема

Все неприводимые многочлены n-й степени из $\mathbb{F}_p[x]$ делят многочлен $x^{p^n} - x$.

Доказательство

$n = 1$. *Убеждаемся, что $(x - a) \mid (x^p - x)$, где $a \in \mathbb{F}_p$: при $a = 0$ это очевидно, а в остальных случаях доказано, что a — корень многочлена $x^{p-1} - 1 = (x^p - x)/x$.*

Разложение многочленов на неприводимые

Теорема

Все неприводимые многочлены n-й степени из $\mathbb{F}_p[x]$ делят многочлен $x^{p^n} - x$.

Доказательство

$n = 1$. *Убеждаемся, что $(x - a) \mid (x^p - x)$, где $a \in \mathbb{F}_p$: при $a = 0$ это очевидно, а в остальных случаях доказано, что a — корень многочлена $x^{p-1} - 1 = (x^p - x)/x$.*

$n > 1$. *Строим по неприводимому и (без ограничения общности — нормированному) многочлену $f(x)$ степени n поле $\mathbb{F}_p^n$. В этом поле $\overline{x}$ — корень и $f(x)$, и $x^{p^n-1} - 1$, причём $f(x)$ — м.м. для него.*
По свойствам м.м. $x^{p^n-1} - 1$ делится на $f(x)$.

Пример: разложение $x^{15}+1 \in \mathbb{F}_2[x]$

Проверяем степени 2:

$$2^4-1=15|15, \quad 2^3-1=7 \not| 15, \quad 2^2-1=3|15, \quad 2^1-1=1|15,$$

1. $x(x^{15}+1)=x^{2^4}+x$, откуда все неприводимые многочлены 4-й степени будут делителями $x^{16}+x$ и, следовательно, $x^{15}+1$. Таких многочленов 3:
$$x^4+x+1, \quad x^4+x^3+1 \quad \text{и} \quad x^4+x^3+x^2+x+1.$$
2. $x(x^3+1)=x^{2^2}+x$, откуда все неприводимые многочлены 2-й степени будут делителями x^4+x и, следовательно, x^3+1. Такой многочлен только один: x^2+x+1.
3. $x(x^1+1)=x^{2^1}+x$, откуда единственный отличный от x неприводимый многочлен 1-й степени $x+1$ делит x^2+x.

Итого: разложение $x^{15}+1$ на неразложимые над $\mathbb{F}_2$ многочлены —

$$x^{15}+1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

Многочлены над конечным полем...

Теорема

Любой неприводимый многочлен-делитель $x^{p^n-1}-1$ *имеет степень, не превосходящую* n.

Доказательство

Пусть φ *— неприводимый делитель* $x^{p^n}-x$ *степени* k.
Тогда $F \stackrel{\text{def}}{=} \mathbb{F}_p/(\varphi)$ *— поле, которое рассмотрим как векторное пространство над* $\mathbb{F}_p$ *с базисом* $\left\{\overline{1}, \overline{x}, \ldots, \overline{x^{k-1}}\right\}$.

Обозначим $\overline{x}=\alpha$. *Поскольку* $(x^{p^n}-x) \vdots \varphi$, *то в* F *имеем* $\alpha^{p^n}-\alpha=0$.

Любой элемент F *выражается через базис:* $\beta = \sum\limits_{i=0}^{k-1} a_i \alpha^i$.

Многочлены над конечным полем...

Возведя обе части этого равенства в степень p^n, *получим*

$$\beta^{p^n} = \left(\sum_{i=0}^{k-1} a_i \alpha^i\right)^{p^n} = \sum_{i=0}^{k-1} a_i \alpha^i = \beta,$$

т.е. β — *корень уравнения*

$$x^{p^n} - x = 0\,. \qquad (*)$$

Итак, каждый элемент поля F *является корнем* $(*)$, *но у* $(*)$ *не более* p^n *различных корней, а* $|F| = p^k \;\therefore\; n \geqslant k.$

Многочлены над конечным полем...

Утверждение

Пусть $\beta \in \mathbb{F}_p^n$ *имеет порядок* l, *а его м.м.* $m(x)$ *имеет степень* k.

Тогда ❶ $(p^k - 1) \vdots l$, *а если* $r < k$, *то* ❷ $(p^r - 1) \not\vdots l$.

Многочлены над конечным полем...

Утверждение

Пусть $\beta \in \mathbb{F}_p^n$ *имеет порядок* l, *а его м.м.* $m(x)$ *имеет степень* k.

Тогда ❶ $(p^k - 1) \vdots l$, *а если* $r < k$, *то* ❷ $(p^r - 1) \not\vdots l$.

Доказательство

❶ *По неприводимому многочлену* k*-й степени* $m(x)$ *строим поле из* p^k *элементов. Все его ненулевые элементы, в том числе и* β, *являются корнями уравнения* $x^{p^k-1} - 1 = 0$, *т.е.* $\beta^{p^k-1} - 1 = 0$ *и* $\beta^{p^k-1} = 1$, *но* $\deg \beta = l \Rightarrow l \mid (p^k - 1)$.

❷ *Пусть* $(p^r - 1) \vdots l$ *и* $r < k$. *Тогда* β *— корень уравнения* $x^{p^r} - 1 = 0$, *а т.к.* $m(x)$ *— м.м. для* β, *то* $(x^{p^r} - 1) \vdots m(x)$ *(было доказано)* $\Rightarrow$ *найден неприводимый делитель* $x^{p^r} - 1$ *степени* k, *но* $k > r \Rightarrow$ *противоречие доказанному ранее.*

Многочлены над конечным полем...

Следующая теорема позволяет раскладывать многочлены на множители.

Теорема (свойство корней неприводимого многочлена)

Пусть β — корень неприводимого многочлена $f(x)$ степени n с коэффициентами из $\mathbb{F}_p$. Тогда элементы $\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{n-1}}$:
❶ *все различны;* ❷ *исчерпывают список всех n корней $f(x)$ (их называют смежными).*

Т.е. чтобы получить все корни неприводимого многочлена, достаточно найти один из них и возводить его последовательно в степень p.

Многочлены над конечным полем...

Следующая теорема позволяет раскладывать многочлены на множители.

Теорема (свойство корней неприводимого многочлена)

Пусть β — корень неприводимого многочлена $f(x)$ степени n с коэффициентами из $\mathbb{F}_p$. Тогда элементы $\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{n-1}}$:
❶ *все различны;* ❷ *исчерпывают список всех n корней $f(x)$ (их называют смежными).*

Т.е. чтобы получить все корни неприводимого многочлена, достаточно найти один из них и возводить его последовательно в степень p.

Доказательство

❶ *Покажем, что если β — корень $f(x)$, то β^p — тоже корень.*

Многочлены над конечным полем...

Поскольку $a^p = a$ *для всех* $a \in \mathbb{F}_p$, *то справедливо*

$$\begin{aligned}\left(a_0 + a_1 x + \ldots + a_k x^k\right)^p &= a_0^p + a_1^p x^p + a_2^p x^{2p} + \ldots + a_k^p x^{kp} = \\ &= a_0 + a_1 (x^p) + a_2 (x^p)^2 + \ldots + a_k (x^p)^k,\end{aligned}$$

т.е. для любого многочлена $\varphi(x) \in \mathbb{F}_p[x]$ *выполняется равенство*

$$\left(\varphi(x)\right)^p = \varphi(x^p). \qquad (*)$$

Отсюда:

$$f(\beta) = 0 \;\Leftrightarrow\; f(\beta)^p = 0 \;\Leftrightarrow\; f(\beta^p) = 0$$

и $\beta,\ \beta^p,\ \ldots,\ \beta^{p^{n-1}}$ *— корни многочлена* $f(x)$.

Многочлены над конечным полем...

❷ *Осталось доказать, что все* $\beta, \beta^p, \ldots, \beta^{p^{n-1}}$ *различны, и тогда (многочлен степени* n *имеет не более* n *корней) можно утверждать, что найдены все корни многочлена* $f(x)$.
Предположим, что $\beta^{p^l} = \beta^{p^k}$ *и без ограничения общности* $l < k$. *Имеем:*

1. $\beta^{p^n} = \beta$;
2. *поскольку*

$$\beta^{p^n} = \beta^{p^k \cdot p^{n-k}} = \left(\beta^{p^k}\right)^{p^{n-k}} = \left(\beta^{p^l}\right)^{p^{n-k}} = \beta^{p^{n-k+l}},$$

то β *— корень уравнения* $x^{p^{n-k+l}-1} - 1 = 0$.

Из теоремы «Все неприводимые многочлены n*-й степени над* $\mathbb{F}_p$ *являются делителями* $x^{p^n} - x$*» получаем* $n - k + l \geqslant n \Rightarrow l \geqslant k$ *— противоречие.*

Многочлены над конечным полем: решение уравнений

Примеры

1. Найти корни неприводимого над $\mathbb{F}_2$ многочлена

$$f(x) = x^4 + x^3 + 1$$

Многочлены над конечным полем: решение уравнений

Примеры

1. Найти корни неприводимого над $\mathbb{F}_2$ многочлена

$$f(x) = x^4 + x^3 + 1$$

Решение.

Один корень получаем немедленно: x (или $\overline{x}$).

По только что доказанной теореме можно выписать остальные:

$$x^2, \qquad x^4 = x^3 + 1, \qquad x^8 = x^6 + 1 = x^3 + x^2 + x.$$

Многочлены над конечным полем: решение уравнений

Примеры

1. Найти корни неприводимого над $\mathbb{F}_2$ многочлена

$$f(x) = x^4 + x^3 + 1$$

Решение.

Один корень получаем немедленно: x (или $\overline{x}$).

По только что доказанной теореме можно выписать остальные:

$$x^2, \qquad x^4 = x^3 + 1, \qquad x^8 = x^6 + 1 = x^3 + x^2 + x.$$

Покажем, что, например, x^2 — действительно корень $f(x)$:

$$f(x^2) = x^4 + x^3 + 1\big|_{x \mapsto x^2} = x^{4\cdot 2} + x^{4+2} + 1\big|_{x^4 \mapsto x^3+1} =$$
$$= (x^3+1)^2 + (x^3+1)x^2 + 1 = x^6 + \cancel{1} + x^5 + x^2 + \cancel{1} =$$
$$= x^6 + x^5 + x^2 = x^2(x^4 + x^3 + 1) = x^2 \cdot 0 = 0.$$

Многочлены над конечным полем: решение уравнений

Примеры

2. Решить уравнение

$$f(x) = x^4 + x^3 + x^2 + x + 1 = 0, \quad f(x) \in \mathbb{F}_2[x].$$

Решение.

Один корень получаем немедленно: это x.

Поскольку $f(x)$ неприводим в $\mathbb{F}_2[x]$, то по доказанной теореме можно выписать остальные его корни:

$$x^2,\ x^4 = x^3 + x^2 + x + 1,\ x^8 = x^6 + x^4 + x^2 + 1 = \ldots = x^3.$$

Покажите самостоятельно, что например, x^3 — действительно корень $f(x)$:

$$f(x^3) = x^{12} + x^9 + x^6 + x^3 + 1 = \ldots = 0.$$

Как решать уравнения $f(x) = 0$, когда корней нет?

Алгоритм нахождения всех корней полинома $f(x) \in \mathbb{F}_p[x]$

1. Разложить $f(x)$ на неприводимые множители над $\mathbb{F}_p$:
$$f(x) = g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_k(x).$$

2. Для каждого многочлена $g_i(x)$, $i = \overline{1,k}$ рассмотреть расширение $\mathbb{F}_p[x]/(g_i(x))$, в котором он будет иметь $\deg g_i$ корней
$$\alpha,\ \alpha^p,\ \alpha^{p^2},\ \ldots,\ \alpha^{p^{\deg g_i - 1}}.$$
Записать данные корни как многочлены из $\mathbb{F}_p[x]/(g_i(x))$.

3. Объединить все корни в одном общем расширении $\mathbb{F}_p^m$, где $m = \text{НОК}\,(\deg g_1, \deg g_2, \ldots, \deg g_k)$.

Решение уравнения «многочлен»$= 0$

Задача. Решить уравнение $f(x) = 2x^4 + x^3 + 4x^2 + 4 = 0$, где $f(x) \in \mathbb{F}_5[x]$.

Решение уравнения «многочлен»$= 0$

Задача. Решить уравнение $f(x) = 2x^4 + x^3 + 4x^2 + 4 = 0$, где $f(x) \in \mathbb{F}_5[x]$.

Решение. Вычисляем значения $f(x)$ для $x \in GF(5) = \{0, 1, 2, 3, 4\}$:

$$f(0) = 4, \qquad f(1) = 1, \qquad f(2) = 0.$$

Таким образом, $x = 2$ — корень $f(x)$.
Деля «уголком» $f(x)$ на $f_1(x) = x - 2$ (или на $x + 3$), получим $2x^4 + x^3 + 4x^2 + 4 = (x - 2) \cdot (2x^3 + 4x + 3)$.

Для удобства нормируем частное $2x^3 + 4x + 3$: т.к. $2^{-1} = 3$, то вместо уравнения $2x^3 + 4x + 3 = 0$ будем решать уравнение

$$f_2(x) = 3 \cdot (2x^3 + 4x + 3) = x^3 + 2x + 4 = 0.$$

Решение уравнения «многочлен»$= 0$...

Перебором элементов $x \in GF(5)$ —

$$f(0) = 4, \quad f(1) = 2, \quad f(2) = 1, \quad f(3) = 2, \quad f(4) = 1$$

убеждаемся, что $f_2(x) = x^3 + 2x + 4$ — неприводимый многочлен (а если бы это был многочлен 4-й степени?).

В поле $\mathbb{F}_5[x]/\left(x^3 + 2x + 4\right)$ корни многочлена $f_2(x) = 0$ суть

$$x,\ x^5,\ x^{25} \quad \text{и, кроме того,} \quad x^3 = -2x - 4 = 3x + 1.$$

Вычисляем:

$$x^5 = x^2(3x + 1) = 3x^3 + x^2 = 4x + 3 + x^2 = x^2 + 4x + 3.$$

$$x^{25} = \left(x^5\right)^5 = \left(x^2 + 4x + 3\right)^5 = x^{10} + 4^5x^5 + 3^5 = \\ = x^{10} + 4(x^2 + 4x + 3) + 3$$

(поскольку $4^5 = 2^{10} = 1024$ и $3^5 = 81 \cdot 3 = 243$).

Вычислим отдельно x^{10}.

Решение уравнения «многочлен»$= 0$...

$$x^{10} = \left(x^5\right)^2 = \left(x^2+4x+3\right)^2 = x^4+x^2+3^2+3x^3+4x+x^2 =$$
$$= x^4+3x^3+2x^2+4x+4 =$$
$$= 3x^2+x+4x+3+2x^2+4x+4 = 4x+2.$$

Продолжаем:

$$x^{25} = x^{10}+4(x^2+4x+3)+3 =$$
$$= 4x+2+4x^2+x+2+3 = 4x^2+2.$$

Ответ: $\left\{2,\ x,\ x^2+4x+3,\ 4x^2+2\right\}$.

Решение уравнения «многочлен»$= 0$...

Кстати, является ли многочлен $a(x) = x^3 + 2x + 4 \in \mathbb{F}_5[x]$ примитивным?

Решение уравнения «многочлен»$= 0$...

Кстати, является ли многочлен $a(x) = x^3 + 2x + 4 \in \mathbb{F}_5[x]$ примитивным?

Мультипликативная группа поля $GF(5^3)$ состоит из $5^3 - 1 = 124$ элементов.

Определим порядок её элемента x, для которого $x^3 = 3x + 1$.

Поскольку $124 = 2^2 \cdot 31$ имеет простые делители 2 и 31, равенство $x^d = 1$ нужно проверить для $d = \frac{124}{2} = 62$ и $d = \frac{124}{31} = 4$.

Ясно, что $x^4 = x^3 x = 3x + 1$.

Далее, $x^{62} = (x^{31})^2 = (x^{25} \cdot x^6)^2$.

Поскольку $x^6 = \left(x^3\right)^2 = (3x+1)^2 = 4x^2 + x + 1$, то

$$x^{31} = (4x^2+2)\cdot(4x^2+x+1) = x^4+4x^3+4x^2+3x^2+2x+2 =$$
$$= x^4+4x^3+2x^2+2x+2 = 3x^2+x+2x+4+2x^2+2x+2 = 1$$

— достаточно: $\deg x = 31$ и многочлен $a(x)$ не примитивен.

Решение уравнения «неприводимый многочлен»$= 0$

Задача. Решить уравнение $f(x) = x^2 + 2x - 1 = 0$, где $f(x) \in \mathbb{F}_3[x]$.

Решение уравнения «неприводимый многочлен»$= 0$

Задача. Решить уравнение $f(x) = x^2 + 2x - 1 = 0$, где $f(x) \in \mathbb{F}_3[x]$.

Решение. $GF(3) = \{0, 1, 2\}$.
Перебором элементов $x \in GF(3)$ убеждаемся $f(x)$ — неприводимый многочлен.
Но тогда он имеет корни x и x^3.
Поскольку $x^2 = -2x + 1 \equiv_3 x + 1$, то $x^3 = x^2 + x = 2x + 1$.

Убедимся, что $2x + 1$ — корень $f(x)$:

$$f(x^2 + x) = (2x + 1)^2 + x + 2 - 1 =$$
$$= x^2 + x + 1 + x + 1 = 3 \cdot (x + 1) = 0.$$

Решение уравнения «неприводимый многочлен»$= 0$...

Проверим, кстати, является ли многочлен $f(x) = x^2 + 2x - 1 \in \mathbb{F}_3[x]$ примитивным?

Мультипликативная группа поля $GF(3^2)$ состоит из 8 элементов, $8 = 2^3$ имеет единственный простой делитель 2 и поэтому необходимо проверить равенство $x^4 = 1$.

Имеем $x^2 = x + 1$ и

$$x^4 = \left(x^2\right)^2 = (x+1)^2 = x^2+2x+1 = x+1+2x+1 = 2 \neq 1.$$

Это означает, что $\deg x = 8$ и данный многочлен — примитивный.

Разделы

Разделы

Разделы